DISEÑO DE UN MARCO METODOLÓGICO PARA LA GESTIÓN DE RIESGOS DE TI PARA EL GRUPO EMPRESARIAL JADE.

LILIBETH NAVARRO BERNAL
HENRY PALOMINO CATALAN

Proyecto presentado como requisito para optar el titulo de Magister en Gobierno de Tecnología Informática.

Tutor: JORGE ALBERTO GIL PEÑALOZA

FUNDACION UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRIA PROFESIONAL EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA – COLOMBIA
2010

TABLA DE CONTENIDO

TABLA DE FIGURAS

TABLA DE SIGLAS

TI: Tecnologías de la Información.
JADE: Acrónimo creado a partir del nombre de los hijos de los socios fundadores.
GobIT: Gobierno de Tecnologías de la Información.
B2C: Business to Costumer.
B2B: Business to Business.
GERTI: Gestión estratégica de Riesgos de Tecnologías de la Información.
COSO: Committee of Sponsoring Organizations of the Tread way Commission
ITGI: IT Governance Institute

1. Agradecimientos

Agradecemos a las personas que nos apoyaron durante nuestros estudios y especialmente a quienes nos dirigieron durante el desarrollo de la tesis: Ing. Jorge Alberto Gil Peñaloza, tutor de este proyecto.

A todo el personal en la Dirección del programa de Maestría de la Universidad Del Norte por su apoyo y confianza.

A nuestras familias por ser nuestra fuerza, apoyo y fuente de motivación e inspiración permanente.

Gracias a Dios, por acompañarnos.

2. JUSTIFICACIÓN

Como es bien conocido a través de la literatura sobre el tema, las grandes empresas en la actualidad se hacen más competitivas dentro de su ramo y adoptan nuevas estrategias a fin de garantizar el éxito.

Estás implementando herramientas de optimización, basadas en las nuevos enfoques gerenciales, gestión estratégica y modelos de medición de gestión, a fin de alcanzar el éxito a corto, mediano y largo plazo con el propósito de establecerse metas que permitan el alcance de los Planes Estratégicos del Negocio, enfocados al cumplimiento de la Visión, Misión, Valores etc., elementos que conjugados comprometen a todos los empleados a la identificación con la organización, a través de un sentimiento de compromiso para alcanzar los objetivos de la misma.

El siguiente se trata de un proyecto de carácter académico que busca enlazar los intereses investigativos con el interés corporativo, fundamentados en la importancia de la gestión de los riesgos actual y, de esta manera, contribuir al desarrollo del área de TI del Grupo Empresarial JADE.

La propuesta se orienta a plantear un marco metodológico para la gestión de riesgos del área de TI, a través de la conexión de marcos de referencia de Gobierno de TI y Administración de Riesgos, con la misión identificar la exposición en los procesos críticos seleccionados, establecer el tratamiento de dichos riesgos y de proponer la estructura para la unidad de gestión de riesgos de TI, inexistente a la fecha.

2.1 ¿POR QUÉ LA GESTIÓN DE RIESGOS?

Hoy día, la gestión de riesgos forma parte de las prioridades para la alta Dirección de las compañías, en procura de dar una respuesta adecuada a su entorno, cada vez más complejo e incierto. En consideración de los autores de este documento, las empresas están asignando recursos específicos para gestionar los riesgos, con un nivel de responsabilidad y capacidad de respuesta apropiados. Así, en grandes compañías se ha creado la figura del Director de Riesgos, para cuyo éxito en el desempeño se exige, además de reportar al máximo nivel de la organización, experiencia y conocimiento suficiente para ser capaz de analizar el negocio desde una perspectiva global, tanto estratégica como operativa.

La gestión de riesgos puede realizar una enorme contribución ayudando a la organización a saber cómo enfrentar los riesgos que pueden afectarle para poder alcanzar sus objetivos. De esta manera, se incrementa el entendimiento de riesgos claves y sus implicaciones, lo que fortalece al negocio y lo hace más competitivo.

La gestión de riesgos permite prepararse buscando asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas. En conclusión, la Gestión de Riesgos ayuda a una entidad a llegar al destino deseado, evitando sorpresas por el camino.

Por consiguiente, estamos en una nueva era de la gestión de riesgos: hoy día los controles, entendidos como todo aquello que procura el logro de los objetivos, son el remedio para el riesgo y el término se aplica a todos y cada uno de los procesos, procedimientos, aplicaciones y datos para la mitigación de riesgos de una empresa.

2.2 ¿POR QUÉ LA GESTIÓN DE RIESGOS DE TI?

Tal como se menciona Luis Fuertes, Marketing Manager de Symantec[1], la mayoría de las compañías, apenas están al tanto de los peligros que corren sus sistemas informáticos, pero muchas no explotan en su totalidad las herramientas que existen para gestionar dichas situaciones, ni tampoco han comenzado a implementar los conocimientos y los procesos necesarios para gestionar este tipo de riesgos. Por ende se han encontrado con un campo nuevo, la gestión de riesgos TI; además de esto, las corporaciones suelen tener un conocimiento muy limitado del impacto que puede tener la pérdida de los bienes informáticos o la imposibilidad para acceder a sus aplicaciones o información. Por ejemplo, la capacidad para transferir riesgos es un concepto fundamental en materia de riesgos financieros; sin embargo, como en los mercados líquidos no es posible todavía comprar y vender riesgos informáticos, las corporaciones deben crear sus propias competencias internas para gestionar este tipo de situaciones por sí mismas [1].

Asimismo, los riesgos informáticos son más difíciles de cuantificar. En TI, aún no existe el tipo de modelo actuarial o estadístico avanzado que valora los riesgos financieros para darles un nivel de precisión razonable. Sin embargo, los puntos

[1] SYMANTEC. Corporación internacional que desarrolla y comercializa software en el dominio de la seguridad informática. Symantec opera en más de cuarenta países.

de vista basados en la heurística y en la experiencia ofrecen unas medidas precisas, valiosas y utilizables de los riesgos informáticos.

Por todo lo expuesto, resulta la necesidad latente de un modelo de Gestión de Riesgos de TI que cubra tanto los aspectos conocidos o clásicos como aquellos no convencionales, y por consiguiente una Administración de los riesgos exitosa en procura de llevar al cumplimiento de las Estrategias de TI y a las de la organización en general sin mayores inconvenientes.

2.3 ¿POR QUÉ EL GRUPO EMPRESARIAL JADE?

Acorde con lo mencionado en uno de los informes de Administración de riesgos de SYMANTEC IT Risk Management Report 2: Myths and Realities [2], las compañías de todo el mundo están analizando detenidamente la administración del riesgo, en este proceso están redefiniendo el rol de la administración del riesgo en cuanto al logro de los objetivos y eventualmente en la generación de valor para los accionistas.

Por supuesto, no existe nada nuevo en el uso de los conceptos de riesgo para la toma de decisiones. Sin embargo, la consideración del riesgo en toda la organización marca una nueva tendencia, incluyendo el desarrollo de planes integrales de administración de riesgos para cubrir estratégicamente todos los procesos de negocios más importantes.

Nuestra propuesta plantea un marco metodológico de Administración de Riesgos para el área de TI, que contendrá una guía para la identificación y detección de riesgos, y donde se propondrán políticas y una nueva estructura organizativa.

En este sentido, en el Grupo Empresarial JADE, la gestión de riesgos de TI toma una importancia crucial, ya que expuesta su situación actual encontramos que es necesario crear programas de gestión del riesgo de TI que consideren la combinación de una amplia gama de riesgos específicos relacionados con la tecnología dentro de un programa de gobierno de TI donde, anticipándose a este tipo de situaciones, se da sentido a la gestión de riesgos de TI desde una perspectiva organizacional, más que centrarse únicamente en la generación de una serie de medidas puntuales que mitigan ciertos riesgos tecnológicos.

3. ANTECEDENTES

Dado que el propósito de este trabajo, además de constituir un requisito para optar el titulo de Magister en Gobierno de TI, consiste en llevar a cabo el diseño de un marco metodológico para la gestión de riesgos de TI para el Grupo Empresarial JADE; en primera instancia, se considera pertinente proponer dicho marco, poner en marcha parte de él y presentar un plan para la implementación de las fases restantes que, dado el alcance de este trabajo, se ejecutarían posteriormente. Comenzaremos por orientar al lector respecto de la organización objeto de este estudio, que es el Grupo Empresarial JADE.

3.1 GENERALIDADES DEL GRUPO EMPRESARIAL JADE

El Grupo empresarial JADE es un grupo de empresas conformado por entidades con inversión privada, dedicadas a la comercialización y distribución de productos en diferentes sectores del mercado nacional [3], así:

- **Distrigras S.A.** cuenta con más de 20 años de presencia en el mercado nacional como concesionario Shell, tiene la distribución autorizada de lubricantes Shell en los departamentos de Atlántico, Magdalena, Cesar, Guajira, Córdoba y Bolívar en las líneas de B2C y B2B.

- **Distribuidora Marsal Ltda** con cerca de 30 años de presencia en el mercado nacional como concesionario Shell, tiene la distribución autorizada de lubricantes Shell en el Valle del Cauca y desde hace 5 años en Nariño, Putumayo, Antioquia y Cundinamarca. En Diciembre de 2008 fue adquirida por el Grupo Empresarial JADE.

- **Dollar King S.A.** dedicada a la comercialización de productos importados y nacionales, tales como: productos para el hogar, decoraciones, ferretería, piñatería, cristalería, aseo personal, labores, entre otros. Utilizando una cadena de 9 puntos de venta con presenta en la costa norte Colombiana. Nace en Marzo de 2007 en sociedad de Caribbean Ventures Inc[2]. En

[2] Caribbean Ventures Inc. Compañía con Sede en Puerto Rico (USA) dedicada a la comercialización en el sector del retail.

diciembre de 2008 fue adquirida la totalidad de sus acciones por el Grupo Empresarial JADE.

3.2 MISIÓN CORPORATIVA

"Generar valor para nuestros accionistas, clientes, colaboradores y vinculados, desarrollando: el Conocimiento del Negocio y del mercado, la Sinergia Empresarial, Manejo de la Tecnología y Procesos." [4]

3.3 VISIÓN CORPORATIVA

"Somos un conjunto de empresas privadas dedicadas a la comercialización y distribución. Compartiendo una misma cultura, principios y valores corporativos que busca un crecimiento constante para el beneficio de sus accionistas, clientes y empleados." [4]

3.4 VALORES CORPORATIVOS

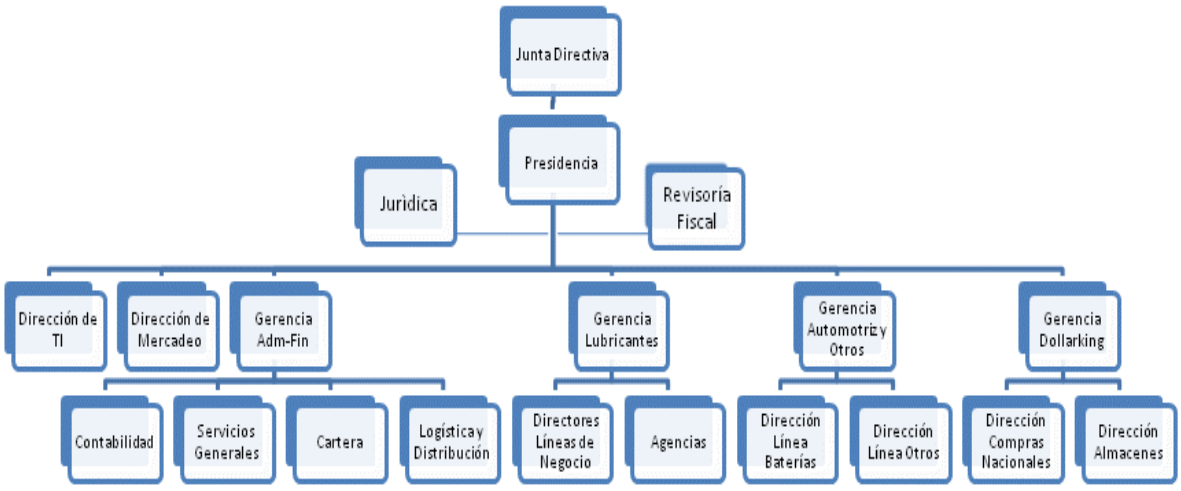
Los valores [4] que rigen la cultura empresarial del Grupo JADE son:

Responsabilidad	Eficiencia
Trabajo en Equipo	Pro actividad
Honestidad	Respeto

3.5 ESTRUCTURA ORGANIZACIONAL

Tiene una estructura organizacional donde se sobrepone una departamentalización por línea de negocio a otra funcional. Es decir, un Director o Gerente funcional que coordina o supervisa el desempeño desde el punto de vista técnico y existe un director o Gerente Ejecutivo que aprovecha lo mejor del equipo y/o empleados en beneficio de la línea de negocio que lidera [5]. En entrevista sostenida con el Gerente Administrativo Financiero destacó que esta estructura facilita la comunicación, estandarización de procesos y el aprovechamiento de los mejores recursos en todas las líneas de negocio.

FIGURA 1 - ORGANIGRAMA GRUPO EMPRESARIAL JADE



4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un Marco Metodológico para la gestión efectiva de riesgos en TI, soportado en estándares internacionales de Gobierno TI, a ser aplicado al Grupo Empresarial JADE.

4.2 OBJETIVOS ESPECIFICOS

- Explorar e Interpretar la Guía Australiana de Riesgo Operativo [6], el Framework RiskIT [7] y la Norma Técnica Colombiana NTC 5254 [8] haciendo de un recorrido a lo largo de los dominios que la conforman y manteniendo los principios que las rigen.

- A partir de dicha exploración:
  - Seleccionar los procesos claves para la efectiva administración de los riesgos de TI en la empresa y preparar los procedimientos y/o diagramas de flujo requeridos para cada proceso.
  - Diseñar un Marco Metodológico de gestión de Riesgos de TI aplicado a la empresa.

- Proponer una nueva estructura organizativa de TI [3], identificando claramente todos los roles, de tal manera que exista una alineación entre las metas de TI y las metas del negocio, basado en los conceptos de Gobierno de TI, los procesos de la organización y el marco metodológico previamente establecidos.

[3] Dicha propuesta estará sujeta a aprobación por parte de las directivas de la empresa.

5. MARCO TEORICO

5.1 DEFINICIONES

GOBIERNO DE TI: responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales. [17]

GESTIÓN DE RIESGOS: un proceso, efectuado por la junta directiva de una entidad, la administración y otras personas, aplicado en el establecimiento de la estrategia y en toda la empresa, diseñado para identificar eventos potenciales que pueden afectar a la entidad, y gestionar los riesgos para estar dentro de su apetito de riesgo, para ofrecer garantías razonables en relación con la consecución de los objetivos de la entidad. [7]

RIESGOS DE TI: Son los riesgos de negocios asociados con el uso, propiedad, operación, la participación, la influencia y la adopción de las TI en una empresa. Se compone de acontecimientos relacionados con TI que potencialmente podría afectar el negocio. Incluye ambos los de frecuencia y magnitud incierta, y crea dificultades en el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de la oportunidades. [7]

APETITO DE RIESGO: Son las actitudes concretas o posición de la organización frente a los riesgos identificados y evaluados una vez se define una cultura organizacional de riesgos[4]. [10]

5.2 GENERALIDADES

Como producto de las estrictas regulaciones sobre el control interno, el riesgo operacional, las responsabilidades de la alta Gerencia y la necesidad de alinear la TI con la estrategia del negocio, los conceptos tradicionales de riesgo, auditoría y control han evolucionado hacia conceptos más amplios como el Gobierno Corporativo y el Gobierno de TI.

[4] Esta definición es la conclusión de los autores con base en las observaciones de varios autores del Instituto de Auditores Internos de Argentina.

Como sugiere Information Systems Audit and Control Association (ISACA)[5] [11]: "Cuando se asume la responsabilidad de gobernar las TI a nivel corporativo, inmediatamente se aceptan muchos retos particularmente interesantes".

El Gobierno de TI como parte integral del Gobierno Corporativo contempla el liderazgo, estructuras de organización y procesos que aseguran que la Tecnología de la Información, soporta los objetivos y estrategias de la organización.

El uso generalizado de las TI no solo puede proporcionar importantes beneficios a una empresa, sino que también implica riesgos. Debido a su importancia de la TI para las empresas, los riesgos deben ser tratados como los demás riesgos empresariales, tales como el riesgo de mercado, riesgo de crédito y los riesgos operativos relacionados con TI. Si bien estos riesgos han sido durante mucho tiempo incorporados a las empresas en los procesos de toma de decisión, muchos ejecutivos tienden a delegar los riesgos a especialistas técnicos de fuera de la sala de juntas.

Por ello los Riesgos asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI dentro de una empresa se convierten en pieza clave dentro del ámbito empresarial y se crea la necesidad de, basados en mejores prácticas y estándares internacionales, buscar mecanismos que permitan la efectiva gestión de los riesgos de TI.

En circunstancias normales, los responsables de seguridad actúan pro activamente para prevenir los efectos perniciosos de los ataques, y cuando no hay más remedio, porque la prevención ha fallado, se actúa a posteriori. Pero, ¿Se plantean los responsables antes de cualquier otra cosa, medir el riesgo que conllevan estas amenazas?

Difícil balanza representa colocar en un lado la cantidad de riesgo que estamos dispuestos a asumir, y el otro lado la cantidad de recursos financieros de los que disponemos para mitigar los riesgos de TI, en especial en materia de seguridad de la información.

Tal como lo menciona VanScoy en *SoftwareDevelopment Risk:Opportunity,Not Problem.* [13]*:*

"El riesgo en sí mismo no es malo; el riesgo es esencial para progresar, y la falla es a menudo una parte clave del aprendizaje. Pero debemos aprender a equilibrar

[5] Asociación Mundial de Ingenieros de Sistemas dedicados a la Auditoría, Control, y seguridad de los sistemas de Información.

las posibles consecuencias negativas de los riesgos contra los beneficios potenciales asociados a su oportunidad."

La administración de los riesgos debe convertirse en parte de la cultura organizacional, de tal manera que esté Integrada dentro de la filosofía, prácticas y planes de negocio de la compañía [7].

5.3 EVOLUCIÓN DE LA GESTIÓN DE RIESGOS DE TI [12]

La gestión de riesgos ha sido objeto de una evolución en los últimos 15 a 20 años. Como la tecnología ha madurado, las formas y medios para gestionar de riesgo han cambiado. Como los ambientes de negocio han cambiado, los riesgos, a su vez, han evolucionado, lo que obligó nuevas exigencias para la tecnología.

La Figura 2 de las edades de la administración de riesgos ilustra la continua puja para cerrar la brecha entre los riesgos, las exposiciones y los procesos de gestión de riesgos. Las prácticas de gestión de riesgos, por naturaleza, siempre han estado ligeramente detrás de la curva cuando se trata de mantener el ritmo de los riesgos.

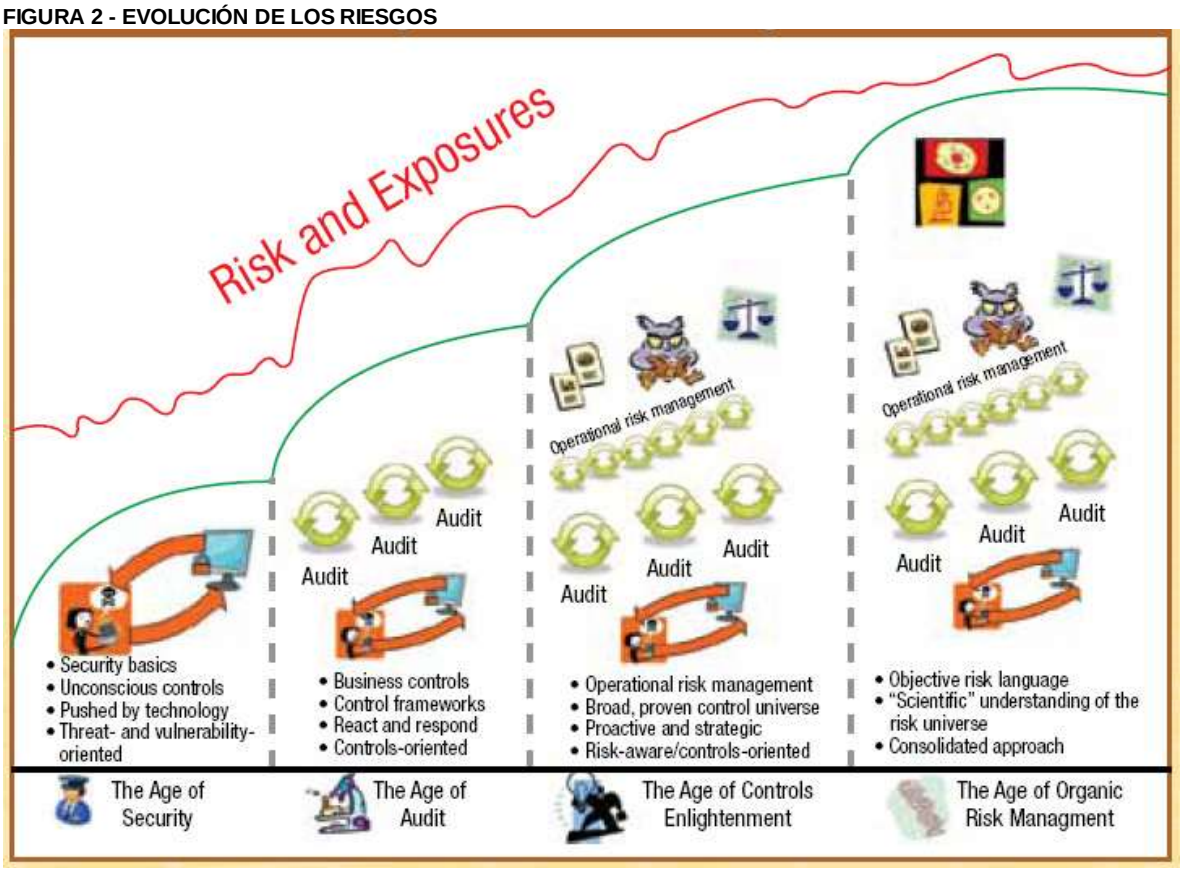
La gestión del riesgo es de esta manera un proceso reaccionario. Si bien hay progreso, siempre parece el riesgo o, más apropiadamente, las amenazas parecen avanzar más en la carrera. En primer lugar, vamos a revisar el pasado para prepararnos para el futuro.

Siempre la gestión de riesgo ha sido una respuesta a los cambios en el entorno de TI, y las edades de los riesgos propuesta por Steve Schlarman se pueden explicar, así:

- En la edad de la seguridad florece el internet y las comunicaciones, se afianza el intercambio electrónico de información y aparecen los hackers concentrándose los riesgos en la confidencialidad e integridad de la información para lo cual la gestión de riesgos inicia como la definición de políticas, funciones y procesos de seguridad.
- En la edad de la Auditoría se expande la infraestructura de TI y se incrementan las inversiones por lo cual TI adquiere un impacto financiero considerable y aparece el Outsourcing de las funciones operativas de TI. Y la respuesta fue las pruebas de auditoría, pruebas de penetración, y aparecen la administración de riesgos en los proyectos de TI.
- En la edad del realce de los controles está en su furor la globalización, surge la explosión de la infraestructura móvil, redes inalámbricas, dispositivos removibles y personales para lo cual se responde con mejoras de gestionando los riesgos orientados al control, Auditorias operacionales y aparecen las primeras estructuras de gobierno y políticas de TI.

- En la edad de la administración de riesgos orgánica hay las más altas expectativas a nivel corporativo sobre la administración de riesgos y el común denominador es la globalización de los servicios y el uso de proveedores de servicio externos, aquí el riesgo se concentra en los requerimientos y regulaciones del entorno y los riesgos de TI se contextualizan como riesgos corporativos para ello la respuesta es programas de administración coordinados en toda la organización y la automatización para el monitoreo de los controles.

FIGURA 2 - EVOLUCIÓN DE LOS RIESGOS



5.4 PRINCIPIOS Y BASES

El Marco Metodológico para la gestión de Riesgos de TI "Marco de Trabajo RiskIT" [7], que plantea el IT Governance Institute ITGI[6], explica los riesgos de TI y ayuda a quienes lo aplican para:

- Una apreciación muy atinada de los riesgos Relacionados de TI presentes y de futuro inmediato, a través de toda la organización y de las bases con las cuales la organización puede atenderlos.

- Una guía punta-a-punta de cómo administrar los riesgos relacionados de TI, más allá del alcance puramente técnico y de sus medidas de control y seguridad.

- Un entendimiento de cómo capitalizar la inversión hecha en un sistema de control interno de TI ya establecido, para administrar los riesgos relacionados de TI.

- Cuando estén evaluando una integración entre la administración de los riesgos de TI, dentro de la administración general de los riesgos empresariales y estructuras de cumplimiento.

- Un marco/lenguaje común para ayudar a gestionar las relaciones entre los responsables ejecutivos de las decisiones (la alta dirección), el Vicepresidente/director de información (CIO) y el administrador del riesgo empresarial, o entre los auditores y la administración.

- Promoción de la responsabilidad del riesgo y su aceptación en toda la empresa.

- Un perfil completo de riesgos para entender mejor los riesgos, a fin de utilizar mejor los recursos de la empresa.

En resumen:

[6] El ITGI es un equipo de investigación y referente líder en gobierno de TI para la comunidad global de negocios. El ITGI tiene por objetivo el de beneficiar a las empresas mediante la asistencia a sus líderes en la responsabilidad para lograr que la TI respalde exitosamente la misión y objetivos de negocios.

- Integrar la administración de los riesgos de TI, dentro de la administración general de los riesgos empresariales y estructuras de cumplimiento.

- Tomar decisiones bien informadas acerca del alcance del riesgo, del apetito al riesgo y su nivel de tolerancia.

- Entender cómo responder al riesgo.

Está dirigido a:

- A la alta Dirección y a sus Comités, quienes necesitan fijar el direccionamiento y monitoreo de los riesgos de toda la organización.

- Gerentes de TI y departamentos de negocio, quienes necesitan definir un proceso de administración de riesgos.

- Responsables y profesionales de administración de riesgos, quienes necesitan guías específicas para el manejo del riesgo de TI.

- Externos Relacionados.

"RiskIT está basado en los principios del Marco metodológico o estándar para la administración de riesgos corporativos tales como COSO ERM [15] y AS/NZS 4360 [6], y provee las instrucciones para aplicar estas guías a TI.

Los Principios del Marco metodológico RiskIT son:

- Gobierno efectivo corporativo de los Riesgos de TI:
    - Siempre conectado a los objetivos de negocio.
    - Alinear la gestión de TI Relacionado a los riesgos del negocio con la gestión de riesgos corporativos.
    - Balancear los costos y los beneficios de la gestión de riesgos.

- Gestión efectiva de los riesgos de TI:
    - Promueve la comunicación abierta y equitativa de los riesgos de TI
    - Establece el tono correcto desde la cima de la organización, mientras esta define y refuerza la responsabilidad personal para operar dentro de unos aceptables y bien definidos niveles de tolerancia.
    - Es un proceso continuo y parte de las actividades diarias

Basándose en estos principios, los pilares fundamentales de una buena gestión de riesgos de TI se definen como sigue:

- Establecer la responsabilidad para la gestión de los riesgos de TI.
- Establecer los objetivos y definir el apetito y tolerancia a los riesgos.
- Identificar, analizar y describir los riesgos.
- Monitorear la exposición al riesgo.
- Tratar los riesgos de TI.
- Enlazar con las guías existentes para gestionar el riesgo.

5.5 FUNDAMENTO DEL RIESGO DE TI

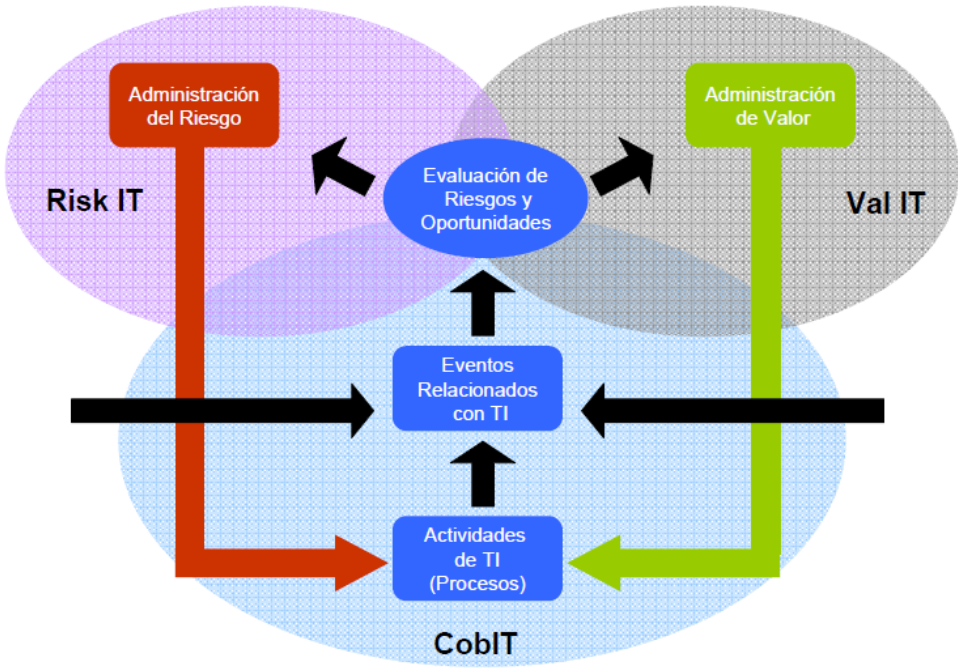
Un primer paso es identificar, entender y evaluar el riesgo de TI considerando todo lo que puede salir mal con o en relación a TI; usando para ello escenarios de riesgo, los cuales contienen varios componentes [7].

FIGURA 3 - ESCENARIOS DE RIESGOS

En el desarrollo de este proyecto, nos basaremos en el Framework RiskIT, la guía Australiana de Riesgo Operativo, y la relación que puede tener este con otros de los estándares internacionales COBIT y Val IT. A continuación se presenta la

relación propuesta por el Framework RiskIT [7] entre el riesgo de TI con COBIT[7] [17] y VAL IT[8] [16]

FIGURA 4 - RELACIÓN ENTRE RISKIT, COBIT Y VAL IT



Existen guías técnicas que complementan el Marco de Riesgo de TI y que proveen ejemplos de posibles técnicas a emplear para su tratamiento, algunas de ellas incluyen:

- Construcción de escenarios a partir de escenarios genéricos de riesgo de TI.

[7] **Control Objectives for Information and related Technology (COBIT)** [17] es un conjunto de mejores prácticas para el manejo de información creado por Information Systems Audit and Control Association ISACA, y el ITGI en 1992. La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados, actualizados, e internacionales para el uso del día a día de los gestores de negocios y auditores. Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las TI.

[8] **Val IT [16]** es un conjunto de documentos que proveen un marco de trabajo para el gobierno de las inversiones en TI, creado por ITGI. Es una declaración formal de los principios y procesos para la administración del portafolio de TI, en concreto, Val IT se centra en la decisión de invertir y la realización de beneficios.

- Construcción de un mapa de riesgos, usando técnicas para describir el impacto y frecuencia de los escenarios.

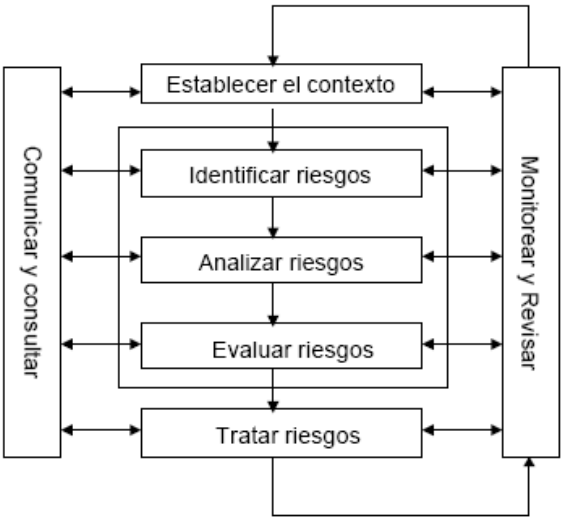
- Construcción de criterios de impacto con relevancia al negocio.

- Uso de COBIT y Val IT para mitigar los riesgos, la liga entre el riesgo y los objetivos de control de COBIT y Val IT, y prácticas clave de administración.

Otro de los complementos para la administración efectiva de los riesgos es la guía Australiana de Riesgo Operativo [6] que provee un instructivo genérico para el establecimiento e implementación el proceso de administración de riesgos involucrando la determinación del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.

Esta guía hace un recorrido a los riesgos, empezando desde su tratamiento e identificación hasta el monitoreo y revisión, lo que le permite a la organización una administración efectiva de los riesgos tanto para evitar o mitigar las posibles pérdidas como para aprovechar las oportunidades que hay en el entorno.

FIGURA 5 – VISIÓN DEL PROCESO DE GESTIÓN DE RIESGOS



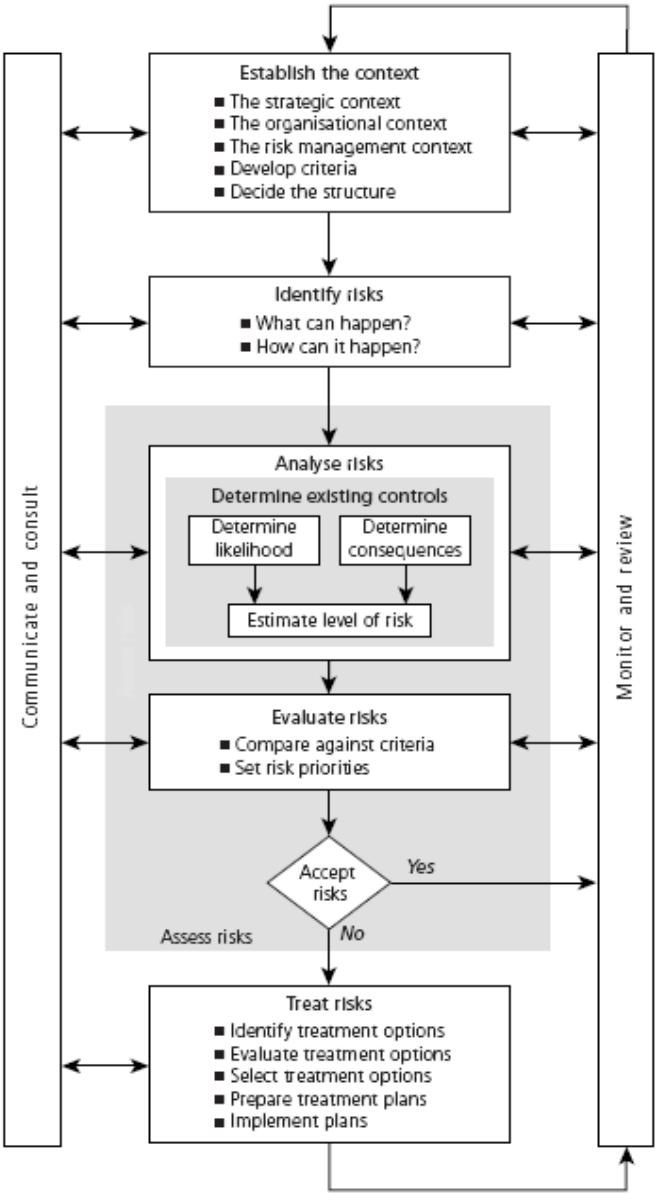
El estándar Australiano presenta una guía práctica para la implementación de un sistema para la administración de riesgos el cual resume en los siguientes pasos:

- Respaldo de la Gerencia
- Desarrollar la política organizacional
- Comunicar la política
- Administrar riesgos a nivel organizacional

- Administrar riesgos a nivel de programa, proyecto y equipo.
- Monitorear y revisar.

Propone el proceso para la gestión de riesgos que se muestra en la figura 6:

FIGURA 6 - PROCESO PARA LA ADMINISTRACION DE RIESGOS



Y consideramos importante el aporte del estándar australiano al presentar los documentos y/o formatos básicos necesarios para lograr una apropiada administración de los riesgos, estos son: El formato para el registro de riesgos, programación para el tratamiento de riesgos y planes de acción para áreas de alto riesgo.

5.6 EL MARCO DE TRABAJO RISKIT

El Marco para la gestión de riesgos "RISKIT" tiene tres dominios: **Risk Governance, Risk Evaluation** y **Risk Response** divididos en 9 procesos de negocio. Cada Dominio contiene a su vez 3 procesos, así [7]:

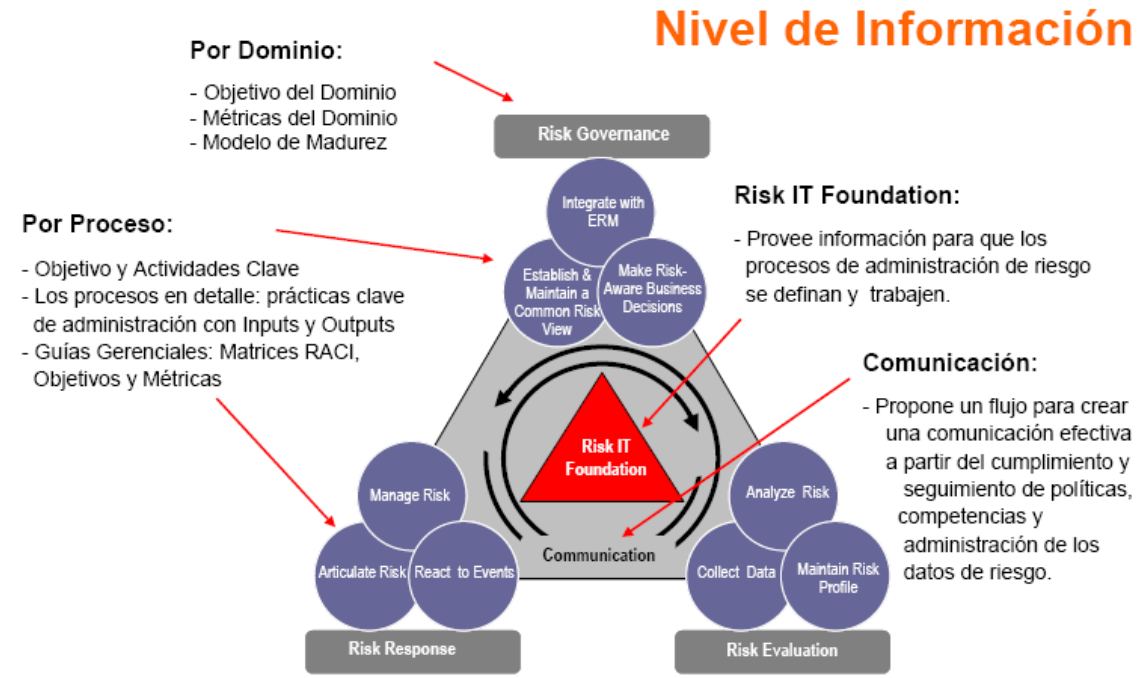
- Risk Governance - RG (Gobierno del Riesgo)
  - Establecimiento y Mantenimiento de una Visión Común de Riesgo
  - Integración con ERM (Enterprise Risk Management)
    Toma de Decisiones de Negocio con una Conciencia del Riesgo
- Risk Evaluation - RE (Evaluación del Riesgo)
  - Recolección de Datos
  - Análisis de Riesgo
    Mantenimiento del Perfil de Riesgos
- Risk Response - RR (Respuesta al Riesgo)
  - Articulando el Riesgo
  - Administrando el Riesgo
  - Reaccionando a Eventos

A manera gráfica el modelo del marco de trabajo ITGI lo representan, así:

FIGURA 7 - COMPONENTES DEL RISKIT

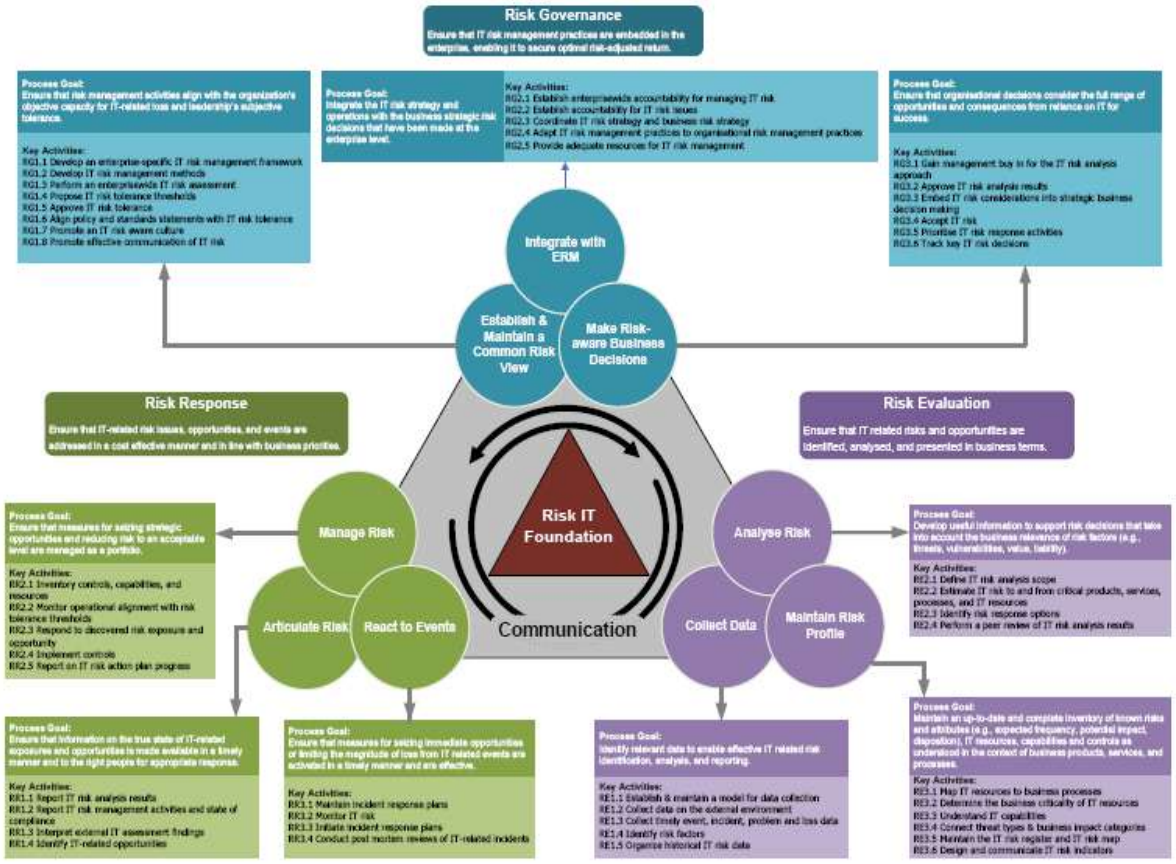
A su vez cada proceso de negocio en cada dominio está conformado por actividades clave y el marco provee Guías Gerenciales (Management Guidelines) que pueden ser usadas para confeccionar los procesos al ambiente de cada organización. Tal como se describe en la siguiente figura [7]:

FIGURA 8 - NIVEL DE INFORMACION POR PROCESO



Para tener una vista general del marco metodológico la ITGI propone la siguiente vista general:

FIGURA 9 - VISTA GENERAL DEL MARCO RISKIT



Además, las Guías Gerenciales que provee el marco de trabajo incluyen Objetivos, Métricas (a diferentes niveles) y Matrices RACI (Responsable, Rendidor de cuentas, Consultado e Informado) por cada uno de los procesos que lo conforman. Y además, para facilitar las comparaciones y benchmarks también existe un modelo de madurez para cada dominio, el cual emplea una escala incremental de 0 a 5.

El Marco para la gestión de Riesgos de TI (RISKIT) define una serie de funciones para la gestión de riesgos e indica donde estas funciones llevan la responsabilidad o rendición de cuentas por una o más actividades dentro de un proceso. Responsabilidad pertenece a los que deben velar por que se completan las actividades con éxito. Rendición de cuentas se aplica a aquellos que poseen los recursos necesarios y tienen la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad específica dentro de los procesos para la gestión de riesgos de TI. La figura 9 es un resumen de los cuadros detallados en el modelo de proceso.

ARQUETIPO DE GOBIERNO DE TI

Partiendo de todo el análisis hecho en este proyecto, podemos decir que la toma de decisiones es un punto clave para alinear TI con el negocio, de allí que una de las herramientas que sirven para catalogar cómo las organizaciones gobiernan las TI es el Modelo de Arquetipos, de Ross y Weill [14].

Dicho modelo propone una matriz que representa gráficamente como se toman las decisiones, y facilita la evaluación, identificación y análisis dónde y de dónde provienen la información para la toma de decisiones en materia de TI.

De acuerdo a lo plasmado por Ross y Weill, el Gobierno de TI abarca cinco grandes decisiones Relacionadas con la administración y uso de TI, que se grafican en las columnas de la matriz. Por otro lado, las empresas utilizan en general seis arquetipos que toman decisiones para decidir; que se representan en las filas de la matriz.

FIGURA 20 – ARQUETIPO DE GOBIERNO DE TI

		Decision Domain									
		IT Principles		IT Architecture		IT Infraestructure Strategies		Bussines Application Needs		IT Investment	
		Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Governance Archetype	Business Monarchy										
	IT Monarchy										
	Federal										
	IT Duopoly										
	Feudal										
	Anarchy										

De manera concreta, según esta propuesta, se dividen las decisiones en TI de la siguiente forma:

1. Principios de TI, o elecciones de alto nivel sobre las TI en la organización.
2. Arquitectura de TI.

3. Infraestructura de TI.
4. Necesidades de negocio (con respecto a las TI).
5. Inversiones en TI y priorización.

Para llegar al análisis de las decisiones de TI los autores del modelo proponen los siguientes interrogantes:

FIGURA 31 – CLAVES PARA LAS DECISIONES DE TI

IT Principles	How do the business principles translate to IT principles to guide IT decisions making? What is the role of IT in the business? What are IT desirable behaviors? How will IT be funded?
IT Architecture	What are the core business processes of the enterprise? How are they related? What information drives these core processes? How must this data be integrated? What technical capabilities should be standardized enterprise-wide to support IT efficiencies and facilitate process standardization and integration? What activities must be standardized enterprise-wide to support data integration? What technology choices will guide the enterprise's approach to IT initiatives?
IT Infrastructure	What infrastructure services are most critical to achieving the enterprise's strategic objectives? What infrastructure services should be implemented enterprise-wide and what are the service-level requirements of those services? How should infrastructure services be priced? What is the plan for keeping underlying technologies up-to-date? What infrastructure services should be outsourced?
Business Application Needs	What are the market and business process opportunities for new business applications? How are strategic experiments designed to assess success? How can business needs be addressed within architectural standards? When does a business need justify an exception to standard? Who will own the outcomes of each project and institute organizational changes to ensure the value?
IT Investment and Prioritization	What process changes or enhancements are strategically most important to the enterprise? What is the distribution in the current IT portfolio? Is this portfolio consistent with the enterprise's strategic objectives? What is the relative importance of enterprise-wide versus business unit investments? Do actual investment practices reflect their relative importance? What is the right balance between top down and bottom projects to balance standardization and innovation?

A lo que con nuestro análisis para el proyecto resumimos como:

Principios de TI. Cómo la tecnología de la Información es empleada en la compañía.
Arquitectura. Organización lógica de datos, aplicaciones e infraestructura capturada en un conjunto de políticas, relaciones y elecciones técnicas para alcanzar la integración y estandarización.
Infraestructura. Servicios centralizados, compartidos y coordinados que proveen la base para la capacidad de la organización de hacer uso de la tecnología.
Necesidades aplicativas. Necesidades de las áreas de negocio respecto a las aplicaciones.

Inversión y priorización. Cuánto y en qué invertir, incluyendo aprobaciones de proyectos y técnicas de justificación.

Por el otro lado, Ross y Weill [14] identifican 6 arquetipos en la toma de decisión en los puntos anteriores, que son:

1. Monarquía de negocio, donde quien decide es el área de negocio.
2. Monarquía de TI, donde quien decide es el departamento de TI.
3. Feudal, donde en cada unidad de negocio/departamento se toman las decisiones de forma individual.
4. Federal, donde las decisiones se toman a nivel organización, pero teniendo en cuenta las diferentes necesidades de las unidades de negocio, es decir, mediante una negociación entre todas ellas.
5. Duopolio, donde se toman en conjunto entre las áreas de negocio y TI.
6. Anarquía, donde todos las toman y nadie reina.

Cada organización tiene un arquetipo general para las cinco diferentes tomas de decisiones, aunque existan excepciones.

El marco metodológico propuesto para el Grupo Empresarial JADE tomará como base estos aspectos, complementados con investigación adicional y la experiencia de los autores de este trabajo.

6. ALCANCES Y LIMITACIONES

6.1 ALCANCES

Los alcances de este proyecto consisten básicamente en lograr diseñar un Marco Metodológico de Gestión de Riesgos de TI para el Grupo Empresarial JADE del sector Comercial de la ciudad de Barranquilla, en un plazo de tiempo de cuatro meses aproximadamente, que incluye las fases de Diagnóstico, Diseño, presentación e Implementación del Marco, sujeto a la aceptación por parte de las directivas de la empresa. Además de esto, se espera aprovechar al máximo cada tutoría, junto con las visitas ocasionales a la empresa, para lograr recopilar toda la información necesaria para la presentación del informe final.

6.2 LIMITACIONES

Con respecto a las limitaciones del proyecto, se encuentra la disponibilidad de tiempo con la que cuente la empresa a visitar, lo cual podría alargar la ejecución del proyecto; sin embargo, para disminuir el riesgo de que esto suceda, se hará la programación de estas actividades con la debida anticipación.

Cabe resaltar que esta propuesta es activa en la medida que se irá validando en el trabajo de campo. Es decir, se irá enriqueciendo continuamente a partir de las experiencias concretas de la realidad, dichas experiencias permitirán la retroalimentación, ajuste y complementación de la programación de actividades de forma continua y permanente.

7. DISEÑO METODOLÓGICO

Consiste en definir la forma como será llevado a cabo el proyecto, indicando el tipo de estudio a seguir y la estrategia general que se utilizará para generar un acercamiento real hacia su objeto de estudio, junto con las características que serán estudiadas y el entorno sobre el cual se concentrará el modelo.

El tipo de estudio que se utilizó para desarrollar el trabajo es de **tipo exploratorio**, ya que procuramos a través de un recorrido detallado hacer un reconocimiento del Framework para la gestión de Riesgos de TI y la guía Australiana; el propósito fue precisar mejor la problemática, nos planteamos interrogantes que nos llevaron a la identificación de los problemas y a la exploración de las áreas afectadas.

El Método de investigación del proyecto, el cual se refiere a los procedimientos que se pueden seguir con el propósito de llegar a cumplir con los objetivos o dar respuesta concreta al problema identificado; fueron aplicados la investigación, observación, inducción, análisis y síntesis.

El primer paso: INVESTIGACIÓN para conocer más a fondo el estado del arte, por medio de la interpretación de buenas prácticas y el marco de trabajo RiskIT y la guía Australiana previamente mencionada.

El segundo paso: OBSERVACIÓN de la situación actual de la empresa, se dio por medio de la percepción de los rasgos existentes, para luego determinar cuál era el estado actual de la empresa frente a la práctica de Gobierno de TI, aplicando las herramientas investigadas en el primer paso. Para ello se programaron visitas casuales para dialogar con algunos directivos de la compañía, a fin de recolectar toda la información necesaria para la realización del trabajo.

El tercer paso: INDUCCIÓN, por medio del cual a través de casos particulares, como situaciones de la empresa, se obtuvieron conclusiones acerca de los procesos requeridos por el Marco de trabajo RiskIT.

En el cuarto paso: ANÁLISIS encontramos la interrelación entre los procesos de JADE contra el Marco de Trabajo RiskIT y la Guía Australiana para, una vez fueron ajustados los procesos, entramos a definir los riesgos en los procesos seleccionados y su tratamiento, como una fase del modelo y

En el quinto paso: SÍNTESIS: se definió el diseño del Marco Metodológico para la gestión de los riesgos de TI, tomando como base las etapas sugeridas por la investigación realizada e integrando los resultados del diagnóstico previamente

mencionado. Finalmente, entramos a proponer una estructura organizacional**,** basada en los principios de Gobierno de TI, para implantar el modelo en cuestión, así como para asegurar su mantenimiento en el tiempo.

En cuanto a las fuentes técnicas de información, para este caso aplicaron los tipos de fuentes primarias y secundarias Relacionadas con el Framework RiskIT, Guía Australiana y la documentación Relacionada con GobIT. De la misma forma se hizo uso de textos, compilaciones de revistas, internet, encuestas, visitas y entrevistas en la empresa según la necesidad.

El proyecto tuvo un periodo de desarrollo de cuatro meses y los componentes para su ejecución constan de cinco etapas, a saber:

Etapa 1: Interpretación del Framework: Consistió en la lectura, análisis y síntesis del marco de trabajo RiskIT, la Guía Australiana y documentos Relacionados con Gobierno de TI. En este caso se realizó una sería de investigaciones y levantamiento de información adicional que permitieron el entendimiento de los procesos y requerimientos de la norma**.**

Etapa 2: Formulación del proyecto: Consistió en la identificación de la situación actual de la empresa frente a la gestión de riesgos y la Gobernabilidad de TI. Se realizaron entrevistas y visitas, de modo que se logró obtener la información necesaria.

Etapa 3: Caracterización de los procesos: Consistió en la identificación de los principales procesos y determinación de las herramientas que se requirieron para seguir las pautas del marco de trabajo.

Etapa 4: Diseño de las Herramientas[9]: En esta etapa se hizo el diseño de las herramientas, teniendo en cuenta los procesos y los conceptos de riesgo operativo.

Etapa 5: Implantación del Marco Metodológico: Parte de la propuesta de la estructura organizacional requerida, y hasta donde fue aprobada la propuesta de implantación de la unidad de GERTI.

[9] Entendiendo como herramientas las que constituyen el modelo que será empleado como Marco Metodológico.

8. IMPACTO Y RESULTADOS ESPERADOS

Este proyecto nace a partir de las necesidades del Grupo empresarial JADE de tomar la administración del riesgo como práctica integral para la gestión de TI. Se espera llegar a diseñar un Marco Metodológico que cumpla con las expectativas de la Gerencia y permita que los objetivos de la Gestión de Riesgos de TI estén alineados con los objetivos del Negocio.

Para alcanzar lo propuesto en el proyecto, se plantearon los siguientes interrogantes, que sirvieron de base para el desarrollo y diseño final:

¿Conoce y/o administra la TI sus riesgos?
¿Podrá la TI adaptarse a los nuevos escenarios?
¿Existe una alineación de objetivos y esfuerzos entre TI y la gestión empresarial?

Buscando responder a estos interrogantes y basados en toda la situación actual, surgió la necesidad de crear un Marco Metodológico que permita:

- Reconocer la existencia de riesgos de TI.
- Facilite la identificación, evaluación y administración de los mismos.
- Reconocer que existe una dependencia muy importante del negocio, hacia el funcionamiento continuo de la TI.
- Identificar y tener claro que si no se implementa un Marco Metodológico para la Gestión de los riesgos, la TI seguiría estando expuesta a riesgos relacionados con: la seguridad de sus sistemas, la continuidad del servicio, los fraudes, daños en la infraestructura, pérdidas o alteraciones de información sensible, multas o penalizaciones, incidentes operativos, daños físicos y ambientales, etc.
- Identificación de nuevas oportunidades de negocio a través del uso de la TI.
- Tomar decisiones bien informadas acerca del alcance del riesgo, y su nivel de tolerancia.
- Cumplimiento presupuestal y atención de requerimientos regulatorios.

9. CRONOGRAMA

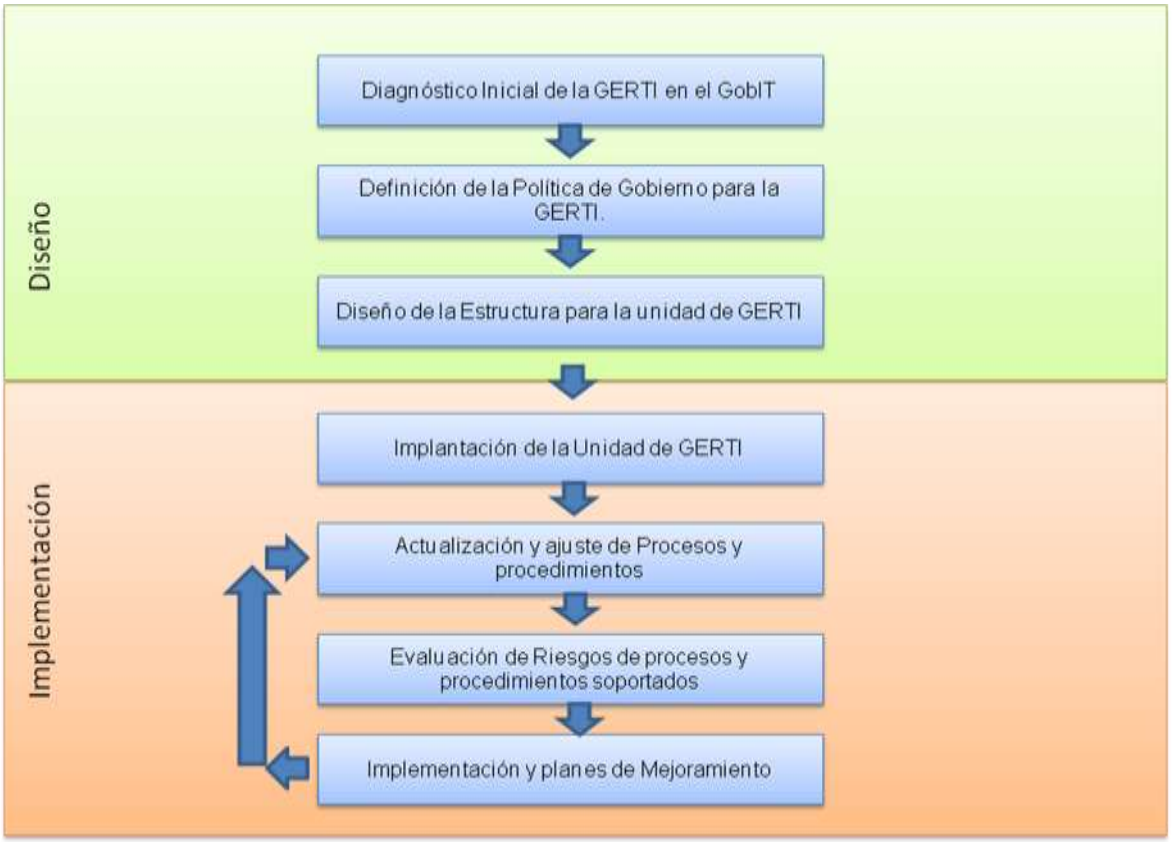
La elaboración de este proyecto se planteó en las siguientes fases:

Fase	Duración
Levantamiento Bibliográfico.	3 Semanas
Recorrido y Análisis del contenido de Marco RiskIT, la Guía Australiana, Marco COBIT y la Norma Técnica NTC 5254.	5 Semanas
Análisis y Evaluación de la situación actual de la empresa	2 Semanas
Diseño del Marco Metodológico de Gestión de Riesgos de TI aplicado a la empresa	3 Semanas
Sujeto a la aprobación de la empresa se Iniciará la Implementación del Marco Metodológico	2 Semanas
Preparación Informe final	1 Semana

10. MARCO METODOLÒGICO PROPUESTO

En primera instancia una representación gráfica de las fases que componen el marco metodológico de GERTI propuesto para el Grupo Empresarial JADE. En el cual, se distinguen dos grandes etapas: Diseño e Implementación que están compuestas por fases secuenciales en la primera y fases que forman un ciclo en la segunda etapa.

FIGURA 12 – MARCO METODOLÓGICO DE GERTI



Empecemos a desarrollar cada una de las fases:

10.1 DIAGNOSTICO INICIAL PARA GOBIT EN EL GRUPO EMPRESARIAL JADE

El desarrollo del Arquetipo de Gobierno de TI [14] sirve para evaluar y comparar el Gobierno de Tecnologías de la Información (TI); para lo cual, proponen una matriz que representa gráficamente como se toman las decisiones.

FIGURA 43 - ARQUETIPO DE GOBIERNO DE TI GRUPO EMPRESARIAL JADE

		Decision Domain									
		IT Principles		IT Architecture		IT Infraestructure Strategies		Bussines Application Needs		IT Investment	
		Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Governance Archetype	Bussiness Monarchy										X
	IT Monarchy				X		X				
	Federal	X				X		X		X	
	IT Duopoly		X	X					X		
	Feudal										
	Anarchy										

Donde identificamos como aplican cada dominio a un arquetipo, así:

Principios de TI: Las solicitudes son realizadas por los líderes de procesos de negocio con lo cual se obtienen decisiones separadas acordes a las necesidades de cada unidad. Dichas decisiones son tomadas conjuntamente por el Director de TI y el Gerente Administrativo.

Arquitectura de TI: Las solicitudes respecto a este dominio son realizadas por un equipo conformado por el Director de TI y el Gerente Administrativo los cuales realizan un estudio a fondo de los procesos base del negocio y tienen una visión global de las capacidades técnicas y actividades son requeridas para soportar la integración del negocio. Las decisiones en este dominio son tomadas por el Director de TI quien escoge la arquitectura y guía las iniciativas de TI.

Infraestructura de TI: Las necesidades de cada unidad son solicitadas por grupos operativos y/o lideres de cada negocio quienes demuestran el grado de criticidad y como se puede cuantificar el valor del requerimiento para que el Director de TI este en capacidad de decidir sobre los planes para mantener y/o una infraestructura. De la misma forma, para que pueda determinar qué servicios puedan ser tercerizados.

Necesidades de aplicaciones de negocio: Los líderes de cada negocio presentan las necesidades de nuevas aplicaciones para aprovechar oportunidades en sus

procesos. Las decisiones son tomadas por un equipo de trabajo entre la Gerencia Administrativa y el Director de TI, quienes definen como serán estratégicamente la forma y el tiempo en que se podrá cubrir esta necesidad.

Inversión y Priorización de TI: Las solicitudes de cambios en los procesos base del negocio y/o cambios en los objetivos estratégicos son solicitados por sus líderes y la decisión está en manos de un equipo Dirección ejecutiva conformado por el Gerente General, Gerente de Línea de negocio, Gerencia Administrativa y el Director de TI, quienes establecen el balance correcto y toman decisiones sobre los proyectos de innovación y estandarización de los procesos de negocio.

En resumen observamos[10] que la mayoría de las decisiones de TI son tomadas por la Dirección de TI. Es decir, en cuanto a las decisiones su GobIT es altamente Centralizada en la Dirección del TI. Sin embargo, las solicitudes están altamente distribuidas y el resto de la organización participa activamente.

Como producto del diagnóstico se determinó que el Grupo empresarial JADE[11] :

Está expuesto a riesgos Relacionados con: la seguridad de sus sistemas, la continuidad del servicio, fraudes, daños en la infraestructura, pérdidas o alteraciones de información sensible, multas o penalizaciones, incidentes operativos, daños físicos y ambientales, entre otros.

Los sistemas aplicativos y su infraestructura: no cubren las expectativas para el negocio o simplemente no son bien aprovechados, por falta de conocimiento profundo.

Ausencia de Gobierno de IT: las prácticas de operación y control de IT son informales, existe mucho re-trabajo, tiempos elevados para realizar mantenimientos de aplicaciones cuellos de botella en proyectos, niveles bajos de calidad en el servicio y deficiente organización de las actividades internas.

El área encargada de TI: vista como un área de 'gasto permanente' y no se muestra aún ningún retorno a la inversión.

El departamento de TI tiene personal debidamente capacitado en tanto en el software y aplicaciones utilizados como soporte a la operación del negocio. A

[10] Las observaciones presentadas corresponden a los resultados del análisis de la matriz elaborada por los autores.

[11] Las afirmaciones presentadas son el resultado del análisis realizado por los autores al hacer un recorrido fundamentado en los objetivos de control de COBIT sobre el estado actual de los servicios de TI en el grupo empresarial JADE.

pesar que el nivel de los usuarios en sus conocimientos en informática no es alto, los sistemas le ofrecen herramientas que apoyan su gestión adecuadamente aunque en ocasiones se perciben retrasos en la toma de decisiones por supuesta falta de información que obedece a la incapacidad de ciertos usuarios de resumir, tabular y analizar la información de forma autónoma, requiriendo del concurso de funcionarios de TI para tal fin.

Además qué, debido a los procesos de fusión de las empresas del Grupo, los miembros de las áreas de negocio no tienen claro cómo abordar los problemas relacionados con TI y definir la responsabilidad de los mismos. En ocasiones la interrelación se desarrolla con ciertos roces entre las partes que participan.

Para las empresas de lubricantes del Grupo se hacen necesarios procesos más integrados y herramientas que permitan extraer la información de manera estructurada y más ágil en las áreas de cartera, inventario y ventas. Para los almacenes y empresas de lubricantes se requiere un mayor nivel de agilidad y detalle en la información de compras a fin que se faciliten la toma de decisiones en estos procesos.

Existen herramientas de Inteligencia de Negocios que apoyan las operaciones de ventas, inventarios y financieros en los almacenes pero es notoria su ausencia en las empresas de Lubricantes.

Los miembros de TI conocen al detalle el entorno de la infraestructura que administran y expresan que necesitan mejorar la seguridad de la LAN en lo que se refiere a sistemas de autenticación y mejor nivel de acceso a los recursos de la red, sobre todo en las sedes remotas las cuales no tienen controlador de dominio activo.

Declaran que no existe un control del inventario de activos y/o infraestructura en la organización. Existen controles básicos: listados y documentos en Excel, pero no existen sistemas de identificación y/o marcado de los equipos, mucho menos herramientas automatizadas para toma de inventario.

De acuerdo al plan estratégico organizacional se pretende dar una mayor atención para mejorar el nivel de servicios y la cultura informática de la organización. En este sentido la empresa espera afrontar muchos proyectos los cuales hasta la fecha no se están administrando una tecnología o modelo estándar del mercado, aunque informalmente se sigue una práctica en la que prevalece el criterio del director ejecutivo y el director técnico de cada proyecto.

Los proyectos de TI están definidos a dos años. Los proyectos a corto plazo no están formalmente documentados.

Debido a la informalidad en la administración de los proyectos varias inversiones no se les ha realizado seguimiento y por ende no se les ha medido su generación de valor para la organización. Aunque existen procedimientos formales para presupuestar ingresos y gastos a todo nivel en el negocio, adolecen de estudios técnicos de viabilidad y de oportunidad para los proyectos que justifiquen la aprobación del gasto haciendo una evaluación posterior que presente los retornos sobre las inversiones en TI.

La organización tiene tercerizado en un 95% los servicios de infraestructura y/o hardware para puntos de venta y puestos de trabajo del personal administrativo. Conjuntamente ofrecen el servicio de mesa de ayuda para la gestión de incidentes Relacionados con Hardware. Tiene servicios de comunicaciones en cada sede, agencia y puntos de venta los cuales se encuentra en un 100% en manos de terceros que a la fecha ofrecen un servicio acorde con las necesidades del negocio. Para lograr esto, el Director de TI debe realizar una revisión periódica, según la duración del contrato, del cumplimiento de los acuerdos de servicio. El Director de TI, durante la operación diaria, de acuerdo a los reportes de incidencias va verificando el cumplimiento de los niveles de servicio y son renegociados de acuerdo al desempeño de cada uno. Por política, la organización no está interesada en adquirir infraestructura y se ha decidido el arrendamiento de infraestructura con el propósito de tener una alta dinámica y rotación de hardware.

Se manejan cláusulas de confidencialidad con todos los terceros; sin embargo, el nivel de información confidencial administrada por terceros es bajo. Todos los equipos son sometidos a técnicas de borrado y formateo básicos de medios de almacenamiento antes de ser entregados y/o devueltos a terceros con el propósito de no comprometer la información del negocio en manos de terceros. Hasta la fecha el servicio ha sido controlado sin mayores trastornos y entregado con un nivel de servicio adecuado y conforme a los niveles acordados. La capacidad tecnológica de los terceros ha estado en buenos niveles y no se han presentado incidentes o retrasos en el servicio debido a la incapacidad de los terceros para responder a las necesidades de la organización.

La entidad debe poner en marcha políticas detalladas para poder valorar adecuadamente si todos los procesos a cargo de TI se pueden externalizar y cómo. La alta dirección es responsable no sólo de esta política sino también de las actividades llevadas a cabo bajo la misma. La entidad debe establecer un programa de gestión de riesgos para la revisión y el control de las actividades externalizadas y las relaciones con los proveedores de servicios. La entidad debe asegurarse de que los acuerdos de tercerización en ningún caso disminuyen la capacidad de cumplir sus obligaciones con clientes y reguladores ni impiden una supervisión efectiva.

La organización, para satisfacer sus necesidades de desarrollo de aplicaciones, trabaja con dos proveedores que son personas naturales, quienes conocen a fondo dos de las aplicaciones pilares (financiera y comercial – compras) pero no poseen una estabilidad financiera adecuada. Las fuentes de los productos de sus contratos quedan a disposición de la empresa para garantizar su continuidad de cambio en el tiempo. A pesar que se conoce la existencia de estándares internacionales para el desarrollo de aplicaciones no se siguen, ni exigen, estás prácticas a los terceros encargados de los desarrollos externos. El análisis de requerimientos es levantado por el área de TI siendo estos los directos responsables del diseño de las aplicaciones con la participación de los terceros involucrados en el proceso. Existe un alto grado de informalidad en los procesos de desarrollo de aplicaciones y la documentación del proceso y el producto final es pobre.

Poseen prácticas generales para el control de cambios.

Se presentan fallas regulares en los procesos de implementación y las fallas son detectadas por los usuarios finales de las aplicaciones al momento de la entrada en producción. En términos generales, los usuarios están satisfechos con las aplicaciones entregadas ya que cumplen las necesidades del negocio.

Se presentan necesidades de información a nivel de mercadeo gerencial en el ámbito financiero y comercial las cuales son cubiertas mediante la elaboración de informes en Excel después de su extracción desde el Datamart de Inventarios y Ventas, el sistema para Control de Presupuesto y ejecución de compras o en su defecto desde archivos planos en el sistema contable.

Muchos de los requerimientos de mercadeo se refieren a promociones las cuales no pueden ser satisfechas y originan el ingreso sin control de descuentos de acuerdo al criterio de los encargados de la facturación.

El nivel de servicio ofrecido por el área de TI es satisfactorio para la organización y por medio de él se garantiza la continuidad del servicio. Se realizan mediciones de la capacidad y tolerancia de los equipos de misión crítica (Servidores, Redes, Sistemas de potencia y respaldo, entre otros) actualmente en operación. Por otro lado, se dispone de planes de contingencia de servidores, equipos en puntos de venta, sistemas de potencia con sus respectivos planes para recuperación ante desastres. Aunque no se realizan las pruebas y simulacros con la frecuencia planeada de la mano con los planes de continuidad del negocio.

Existe un manual de seguridad interno para el negocio el cual no abarca el área de TI ampliamente solo en sus generalidades. No existen controles estrictos de acceso y seguridad del centro de cómputo. Los usuarios son los responsables de la información generada en cada uno de sus maquinas, ya que no existe una

política general para la seguridad de la información creada en la máquina de cada usuario. Existen políticas definidas del software autorizado para usar y se realiza seguimiento periódico para controlar el uso en los equipos de la organización.

Se conocen si los incidentes que se generan diariamente se recogen, analizan y solucionan adecuadamente para que no queden los problemas abiertos y no se vuelvan a repetir. Se determina si los usuarios hacen un buen uso de las aplicaciones y de los equipos. Esto se consigue haciendo seguimiento y tabulación de las incidencias, lo cual sirve para definir los correspondientes planes de formación y concientización.

Existen manuales de operación, preparación de trabajos, control de los procesos batch de las aplicaciones, copias de seguridad de los datos y funcionamiento de los procesos de recuperación. Y además existe control de la integridad de los procesos.

A nivel general la organización tiene un alto nivel de cumplimiento de las obligaciones regulatorias, normatividad legal y a su vez conoce la participación de TI en este índice. No se realizan prácticas de control interno al interior del área de TI pero si se tiene control sobre las autorizaciones y permisos de los usuarios de los sistemas de información de la organización.

No existen procesos formales de auditoría y control interno al interior del área de TI por ende el nivel de auditoría es bajo.

10.1.1 REVISIÓN DE RIESGOS EN PROCESOS CRITICOS SELECCIONADOS

Con base en el análisis de la situación actual y las prioridades planteadas por los miembros de las directivas de la organización se escogieron tres procesos, así:

10.1.1.1 Generalidades de los procesos críticos seleccionados

Adquisición y Tercerización de Infraestructura

El Grupo Empresarial JADE en virtud de obtener una dinámica efectiva que le permitiese ajustar la adquisición de infraestructura a las operaciones y variaciones del negocio adoptó una política de tercerización de la adquisición de infraestructura mediante la figura de arriendo. Los beneficios que ofrece son:

- Disponibilidad de equipos a conveniencia de las necesidades del negocio en cantidad y tiempo de respuesta.
- Posibilidad de ajustar la cantidad de equipos requeridos acorde con la temporada de ventas.
- Mejor uso del flujo de caja ya que invierten en equipos necesarios para su operación misional y no en equipos de apoyo transversal.
- Mayor cubrimiento del departamento de servicio y soporte porque el proveedor se encarga del soporte y mantenimiento de la plataforma instalada.
- Beneficios tributarios por llevar los servicios contratados como gasto.
- Disminución de gastos en depreciación de activos.

Para garantizar la obtención de estos beneficios y alcanzar un adecuado nivel de servicio en la gestión de infraestructura tienen en cuenta:

- Establecer, con la dirección del negocio, los niveles de servicios requeridos para cada área y/o negocio.
- Establecer acuerdos de servicio clasificados en categorías: A, B y C donde se discriminan las características de los equipos y el nivel de servicio de cada categoría.
- Hacer las solicitudes al proveedor de los servicios requeridos de acuerdo a las necesidades de los representantes del negocio en la categoría adecuada.
- Recibir todas las solicitudes de servicio y soporte técnico las cuales son pre-evaluadas y luego enviadas a la mesa de ayuda del proveedor. Según los antecedentes y el diagnóstico se decide si se solicita mantenimiento preventivo, correctivo y/o cambio.
- Solicitar al proveedor la entrega de los servicios y presentación de informes técnicos.
- Conjuntamente con el director de sistemas, realizar revisiones periódicas donde se evalúan el cumplimiento de los acuerdos de servicio y condiciones de negociación (Tarifas).

Gestión de Proyectos

Para el desarrollo de este proceso dentro del Grupo Empresarial JADE se tienen las siguientes actividades:

- De acuerdo a las necesidades presentadas durante el comité ejecutivo por los ejecutivos, los directivos, conjuntamente con la Dirección de Sistemas, deciden cuales proyectos conformaran el portafolio el cual documenta informalmente el Director de Sistemas.

- Una vez aprobada por la Dirección del Negocio la ejecución del proyecto, el Director de Sistemas realiza el análisis de requerimientos.
- Se presenta un diagnóstico detallado de la situación actual del negocio y se presentan posibles soluciones a manera general e informal.
- El Director del Negocio determina las directrices a seguir y da los lineamientos del proyecto.
- El Director de Sistemas realiza el levantamiento y evaluación de alternativas solución y se decide la opción a desarrollar.
- Se inicia la búsqueda y evaluación de proveedores, se escoge el proveedor y se determinan las necesidades de aprovisionamiento, cronograma, recursos y entregables.
- Se desarrolla el aprovisionamiento de acuerdo a las necesidades del proyecto.
- Se inicia el desarrollo por parte del proveedor.
- Se realizan reuniones periódicas de acuerdo al cronograma donde se revisan los entregables.
- Se realizan los programas de capacitación
- Se establecen y desarrollan las pruebas de pre-implantación.
- El proveedor hace la implantación y entrega del proyecto.
- El Director de Sistema recibe las actas de entrega del proyecto y presenta a las directivas y ejecutivos del negocio el proyecto terminado.

Gestión de usuarios para aplicaciones

Para determinar los requisitos y responsabilidades que deben seguir todos aquellos usuarios de las aplicaciones del grupo JADE, con el fin de otorgar acceso a las mismas mediante el uso y asignación de usuarios y contraseñas según el perfil definido, buscando la protección de la confidencialidad, integridad y disponibilidad de la información de la compañía, se establece las siguientes actividades para este proceso:

Este proceso aplica para todas las actividades que requieran conceder acceso a las aplicaciones críticas que son administradas por la Dirección de Tecnologías de Información y que se encuentran listadas en el documento “Lista de aplicaciones con Infraestructura”.

Todos los formatos, autorizaciones y demás documentación que sea utilizada para propósitos de auditoría, se almacenan en formato digital, en la carpeta del sistema de información implicado en el cambio, en el servidor dispuesto para ello, teniendo precaución de identificar claramente los archivos por la fecha del cambio realizado. Se encuentra definida la ruta donde se almacenarán estos formatos y la identificación que debe asignarse.

La solicitud de cuenta de usuario para de acceso a aplicativos administrados por la Dirección de TI debe ser realizada por el director del área a la cual pertenece el funcionario que necesita el acceso. Dicha solicitud se realiza por correo electrónico al líder funcional de la aplicación, adjuntando “Formato de Novedades de Cuentas de Usuario para Aplicaciones”.

El líder funcional que tenga asignada la solicitud, debe evaluar si el requerimiento está completo. Si no cumple con todos los requerimientos se debe gestionar con el solicitante la corrección de la misma. En caso contrario, se crea el usuario según el perfil consignado en el formato y le asigna una contraseña por defecto. De igual manera, se asignan los privilegios asociados al usuario según lo definido en el formato y lo actualiza únicamente con el nombre de usuario asignado. Además, verifica si es necesario realizar alguna instalación en el equipo del usuario, dejando constancia de ello en el formato.

Una vez creado el acceso se informa vía correo electrónico a quien realizó la solicitud y al usuario final con el propósito de dar inicio a las pruebas de la cuenta solicitada.

Para modificaciones de cuentas de usuario, pueden generarse por solicitud del director del área a la cual pertenece el funcionario que necesita la modificación o como resultado de las revisiones periódicas de los permisos de acceso. Se realiza por correo electrónico adjuntando el “Formato de Novedades de Cuentas de Usuario para Aplicaciones”.

El líder funcional que tenga asignada la solicitud, debe evaluar si el requerimiento está completo. Si no cumple con todos los requerimientos se debe gestionar con el solicitante la corrección de la misma. En caso contrario, se realizan las modificaciones aprobadas y se actualiza el formato.

Para eliminación de cuentas de usuario, las solicitudes deben ser realizadas por el director del área a la cual pertenece el funcionario por correo electrónico adjuntando el “Formato de Novedades de Cuentas de Usuario para Aplicaciones”.
El líder funcional que tenga asignada la solicitud debe evaluar si el requerimiento está completo. Si no cumple con todos los requerimientos se debe gestionar con el solicitante la corrección de la misma. En caso contrario, se eliminan los permisos de acceso y se actualiza el formato. En el caso de algunas aplicaciones, el mismo sistema almacena las transacciones realizadas por cada usuario. En este caso la cuenta de usuario no debe ser eliminada sino inactivada, con el fin de no perder el historial de transacciones realizadas por este usuario, dejando constancia de ello en el formato.

Para el desbloqueo de cuentas de usuario, la solicitud debe realizarla el usuario dueño de la cuenta de usuario vía correo electrónico. Luego de confirmar la identidad del solicitante, el líder funcional encargado realiza el desbloqueo.

Para solicitud de cambio de contraseña, la solicitud debe realizarla el usuario dueño de las credenciales de acceso, siempre y cuando el sistema no le permita realizar ésta acción. Luego de confirmar la identidad del solicitante, el líder funcional encargado realiza el cambio.

10.1.1.2 Tablas de impacto

Para los procesos seleccionados, consideramos las siguientes tablas de impacto para los tres tipos de riesgos a evaluar:

Perdida Financiera
5. Perdida del capital de la compañía
4. Perdida del capital de una de las empresas del grupo
3. Perdida del capital de un área de alguna de las empresas
2. Pérdida del valor de una transacción no superior a las anteriores
1. Perdida de un activo

Perdida de continuidad en los servicios
5. más de 4hrs
4. 2 a 4 hrs
3. 30’ a 2 hrs
2. 15’ a 30’
1. menos de 15’

Incumplimiento de objetivos
5. de la compañía
4. de una empresa del grupo
3. de un área de una empresa del grupo
2. de un equipo
1. de una persona

10.1.1.3 Riesgos identificados, controles existentes y controles sugeridos

RIESGO 1. Impacto en la continuidad del servicio debido a la degradación de los servicios por parte del tercero a causa de inestabilidad financiera.

- CE1: Establecimiento de SLA para monitorear calidad de servicio
- CS1: Ampliar el portafolio de proveedores de servicio disminuyendo la dependencia de uno solo.

RIESGO2.Impacto en el cumplimiento de objetivos debido a la falta de estándares para la definición, documentación y ejecución del portafolio de proyectos de TI.

- CS2: Diseñar, elaborar y difundir el documento con el portafolio de proyectos a implementar de forma que permita el seguimiento, auditoría y control de inversiones durante su ejecución.

RIESGO3: Impacto en la continuidad del servicio debido al bloqueo de cuentas de usuarios de áreas misionales.

- CS3: Priorizar atenciones en el proceso de control de cambios.

RIESGO4. Impacto financiero debido a la asignación de recursos a proyectos que no estén alineados con los objetivos estratégicos del negocio.

- CE2: Evaluación de proyectos por el comité de proyectos
- CS4: Establecer procedimientos para listar, priorizar y alinear los proyectos a las estrategias de negocio.

RIESGO5. Impacto financiero debido a la perdida de la confidencialidad de la información por transferencia de cuentas de usuarios.

- CS5: Implementación de mecanismos de control de acceso biométrico

RIESGO6: Impacto en la continuidad debido al incumplimiento del SLA en puntos de venta.

- CS6: Contratación de proveedor de respaldo.

10.1.1.4 Matriz y mapa de riesgos

FIGURA 54 – MATRIZ DE RIESGOS DE TI

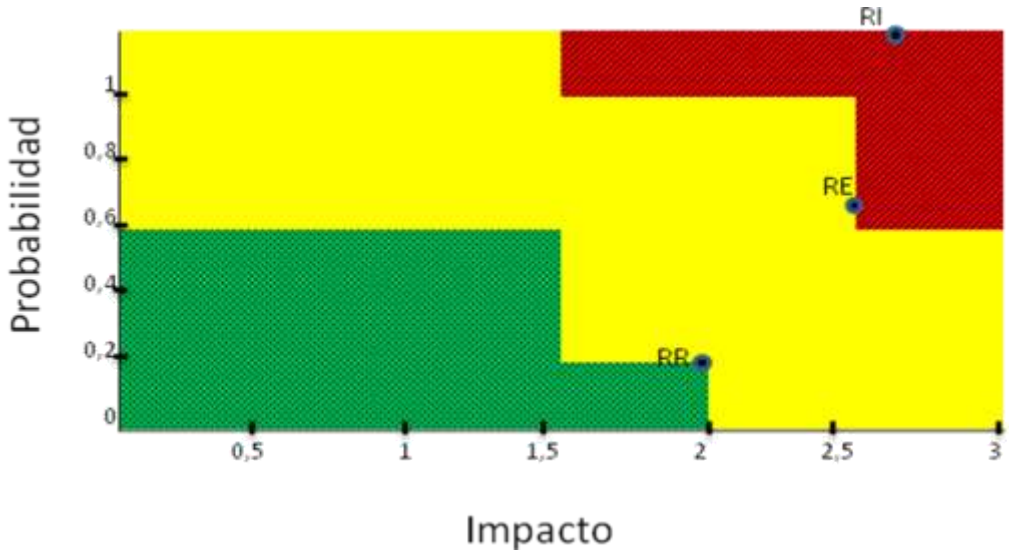
Riesgo	RI		Control Existente	RE		Control Propuesto	RR	
	Impacto	Probabilidad		Impacto	Probabilidad		Impacto	Probabilidad
R1	2	1	CE1	2	0.5	CS1	5	0.1
R2	5	1	NO HAY	5	1	CS2	3	0.2
R3	1	1	NO HAY	1	1	CS3	1	0.1
R4	5	1	CE2	4	0.5	CS4	3	0.2
R5	4	1	NO HAY	4	1	CS5	2	0.5
R6	4	1	NO HAY	4	1	CS6	2	0.5
Total	3.50			2.83			0.63	
Promedio Impacto	3.50			3.33			2.67	
Promedio Probabilidad	1.00			0.83			0.27	

De acuerdo con la matriz de riesgos, los riesgos más relevantes son:

0,1	R3
0,5	R1
0,6	R2
0,6	R4
1	R5
1	R6

El mapa de riesgos definido es:

FIGURA 15 – MAPA DE RIESGOS

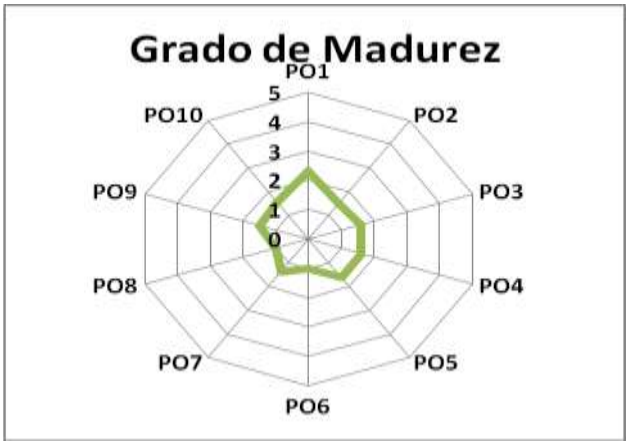


10.1.2 REVISIÓN DE LAS LINEAS DE MADUREZ DE COBIT

10.1.2.1 Evaluación general

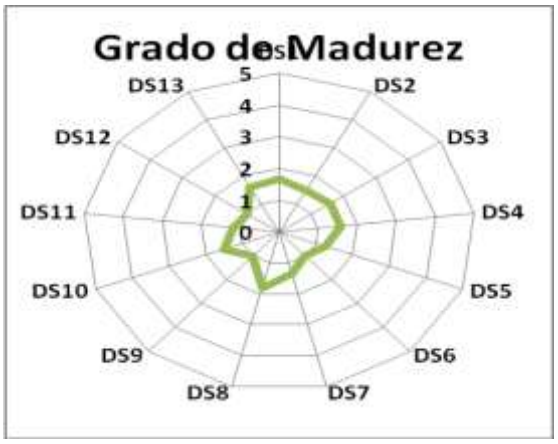
Se realizo la evaluación general utilizando la herramienta para evaluar el nivel de madurez de TI sugerida para tal fin y siguiendo los lineamientos de COBIT y los resultados obtenidos fueron por cada Dominio:

Planear y Organizar



Adquirir e Implementar

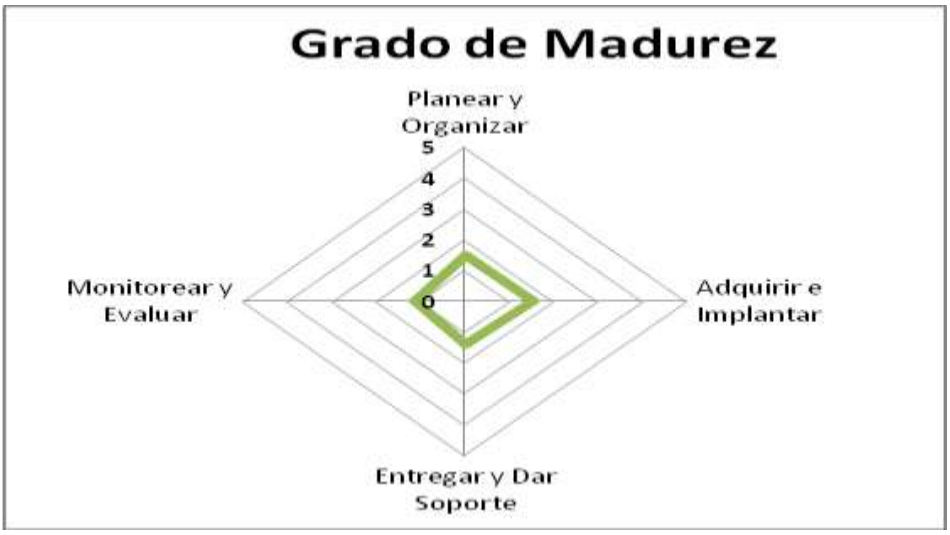
Entregar y Dar Soporte



Monitorear y Evaluar

Y el gran resumen de la evaluación fue:

FIGURA 66 – GRADO DE MADUREZ DE PROCESOS DE DE TI GRUPO EMPRESARIAL JADE



En este encontramos que la Gestión de TI evaluada desde COBIT está en un grado de madurez entre 1 y 2 alrededor de los cuatro dominios que lo componen.

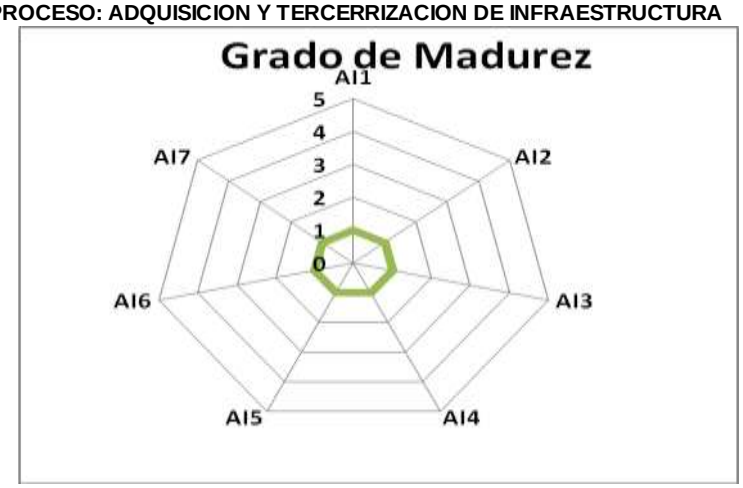
10.1.2.2 Línea de madurez de procesos críticos seleccionados.

Línea de madurez adquisición y tercerización de infraestructura

El dominio al que más se ajusta este proceso es: Adquirir e implementar. El nivel de madurez de este dominio es en promedio 1. Este proceso está Relacionado con la selección de las diferentes infraestructuras requeridas el funcionamiento del negocio.

FIGURA 77 – LINEA DE MADUREZ PROCESO: ADQUISICION Y TERCERRIZACION DE INFRAESTRUCTURA

AI1	1
AI2	1
AI3	1
AI4	1
AI5	1
AI6	1
AI7	1
Total	1



Para lograr un nivel de madurez en nivel 5 en el proceso de este dominio es necesario la definición y el seguimiento de los planes de mejoramiento.

Las actividades recomendadas serian:

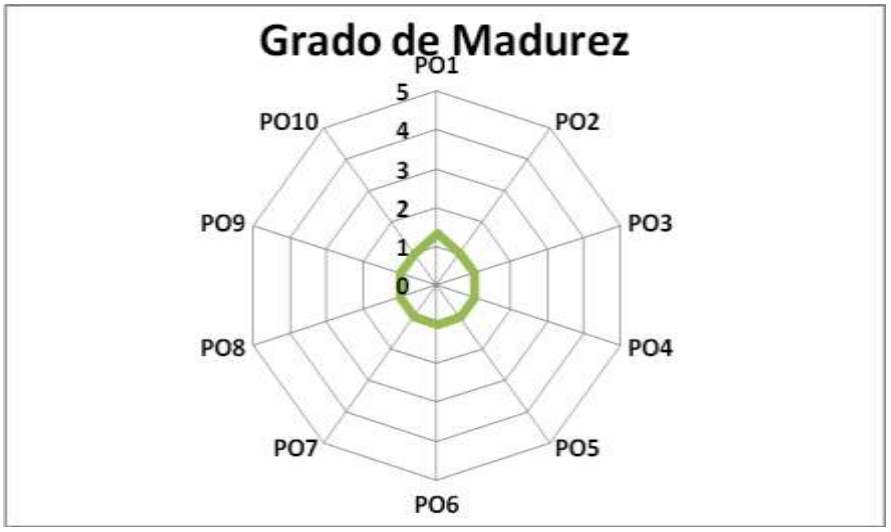
- ✓ Definir un cronograma de monitoreo de la regulación que podría afectar la ejecución del proceso.
- ✓ Definir comité de administración de cambios y de mejora continúa con el fin de optimizar el proceso.
- ✓ Implementar un departamento que regule, controle y haga valer las obligaciones contractuales en la adquisición de infraestructura en sus diferentes modalidades.
- ✓ Realizar un cronograma de capacitaciones que transmita conocimiento a toda la organización sobre una adquisición.
- ✓ Definir responsable de la acreditación de soluciones y cambios a los sistemas.

Línea de madurez gestión de proyectos

El dominio al que más se ajusta este proceso es: Planear y Organizar. El nivel de madurez de este dominio es en promedio 1.

FIGURA 88 – LINEA DE MADUREZ PROCESO: GESTIÓN DE PROYECTOS

PO1	1
PO2	1
PO3	1
PO4	1
PO5	1
PO6	1
PO7	1
PO8	1
PO9	1
PO10	1
Total	**1**



Para lograr el nivel de madurez 5 en el proceso para este dominio es necesario la definición y el seguimiento de los planes estratégicos acompañados de los planes de mejoramiento.
Las actividades recomendadas serían:

- Definir responsable de dirigir y evaluar los planes estratégicos de alto impacto en las estrategias de TI en la organización.
- Definir un procedimiento para priorizar la Administración de la inversión de TI en el presupuesto.
- Definir un responsable de la administración y calidad de los datos relevantes de la empresa.
- Establecer un sistema de gestión de calidad que todo el tiempo este monitoreando el proceso asegurando la calidad del mismo.

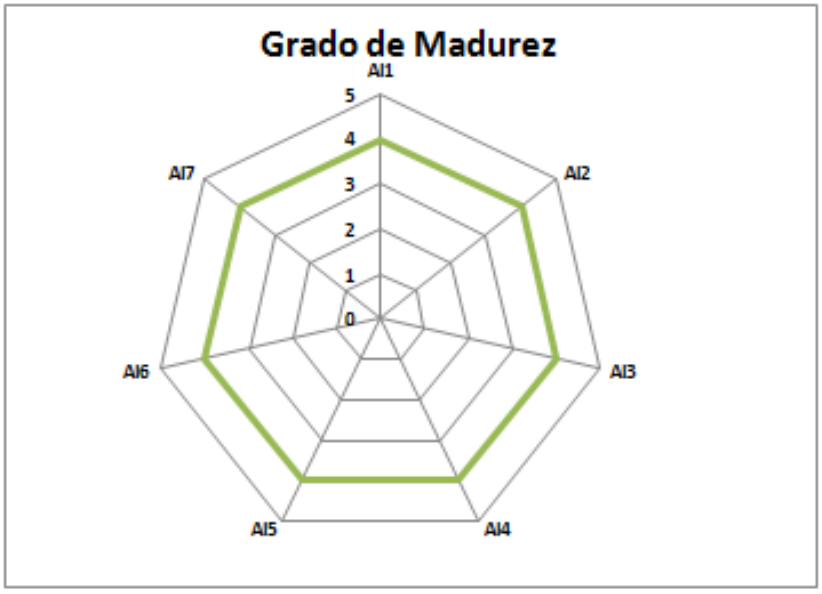
Línea de madurez gestión de usuarios para aplicaciones

El dominio al que más se ajusta este proceso es: *Adquirir e implementar*

El nivel de madurez de este dominio es en promedio 4. Existe una mejor definición de la transferencia del conocimiento en este proceso por cuanto está más asociado con los aspectos de seguridad de la información de la organización lo cual afecta en todos los niveles.

FIGURA 19 – LINEA DE MADUREZ PROCESO: GESTIÓN DE USUARIOS PARA APLICACIONES

AI1	4
AI2	4
AI3	4
AI4	4
AI5	4
AI6	4
AI7	4
Total	4



Para lograr el nivel de madurez 5 en el proceso para este dominio es necesario la definición y el seguimiento de los planes de mejoramiento.

Las actividades recomendadas serían:

- ✓ Elaborar un Plan de Mejoramiento del Proceso, definiendo la periodicidad de la evaluación del proceso mediante el establecimiento de indicadores específicos. Así mismo, definir el procedimiento para realizar el seguimiento al Plan de Mejoramiento producto de la evaluación del proceso.
- ✓ Establecer un procedimiento, preferiblemente automático, que monitoree inactividad de usuarios a fin de detectar posibles retiros sin reporte de cancelación de usuarios a TI.
- ✓ Establecer políticas para el manejo de cuentas temporales (para terceros y/o contratistas).

10.2 DEFINICIÓN DE LA POLÍTICA DE GOBIERNO PARA LA GESTIÓN DE RIESGOS DE TI.

En este contexto se hace necesario que el Grupo Empresarial JADE asuma un compromiso de modernización y progreso en relación con la prevención y gestión de riesgos, introduciendo políticas que inicien y consoliden la prevención y protección de los procesos y recursos de TI en el ámbito de la seguridad.

Teniendo en cuenta los resultados del diagnóstico y basándonos en los principios contenidos en el RiskIT consideramos que los conceptos básicos que deberán tenerse en cuenta para la formulación de una adecuada política de Gobierno para la gestión de riesgos son:

- ✓ Que el Grupo Empresarial JADE tiene el compromiso de cumplir todas las leyes y regulaciones vigentes en cuanto a la seguridad de la información y la gestión de riesgos de TI.
- ✓ Que la Gestión de Riesgos de TI debe constituirse como un eje integrador que atraviese transversalmente todas las actividades y proyectos realizados.
- ✓ Que la declaración de la política de gobierno para la gestión de riesgos de TI debe estar más allá de los cambios de dirección y/o estrategias de gestión. Por tanto, debe perdurar en el tiempo.

- ✓ Que la política de Gobierno para la gestión de riesgos de TI debe ser ampliamente comunicada a nivel de toda la organización.

10.3 DISEÑO DE LA ESTRUCTURA DE LA UNIDAD DE GESTIÓN DE RIESGOS DE TI.

De acuerdo al tamaño, situación actual y necesidades del Grupo Empresarial JADE determinamos que requieren para su unidad de gestión de riesgos de TI una estructura dinámica, que abarque toda la organización y que este alineada para cubrir las necesidades y requerimientos de todas las líneas de negocio. Estando de acuerdo con Henry Mintzberg [18] dice: “Las estructuras burocráticas son demasiado inflexibles y las estructuras simples se encuentran demasiado centralizadas”. “En cambio la Adhocracia es una estructura de proyectos, que incorpora a los expertos que provienen de distintos campos especializados dentro de los equipos creativos que funcionan con armonía e interactúan entre sí".

Fundamentándonos el RiskIT hemos caracterizado los roles para la Unidad de Gestión de Riesgos de TI en el Grupo empresarial JADE, así:

Rol	Definición
Junta Directiva	Los más altos ejecutivos y / o no ejecutivos de la empresa que son responsables de la gestión de la empresa y tener control general de sus recursos
Gerente	El ejecutivo que está a cargo de la gestión total de la empresa
Director de TI	El Responsable de TI, de la alineación de TI y las estrategias empresariales, la planificación, el financiamiento y la gestión de la prestación de servicios de TI y la información y el despliegue de asociados los recursos humanos.
Director Administrativo – Financiero	El Responsable de la Planificación de recursos financieros y administrativos, conservación de documentos, relaciones con los inversores y los riesgos financieros y de la misma forma del recurso humano requerido para las actividades de la empresa.
Comité de Riesgos de la Empresa	El grupo de ejecutivos de la empresa que son responsables de la colaboración a nivel de empresa y el consenso necesario para apoyar a las actividades de gestión de riesgos y decisiones. Puede ser establecido para examinar los riesgos de TI con más detalle y asesorar a la empresa.
Gerente Línea de	Responsables de una línea de negocio especifica, a

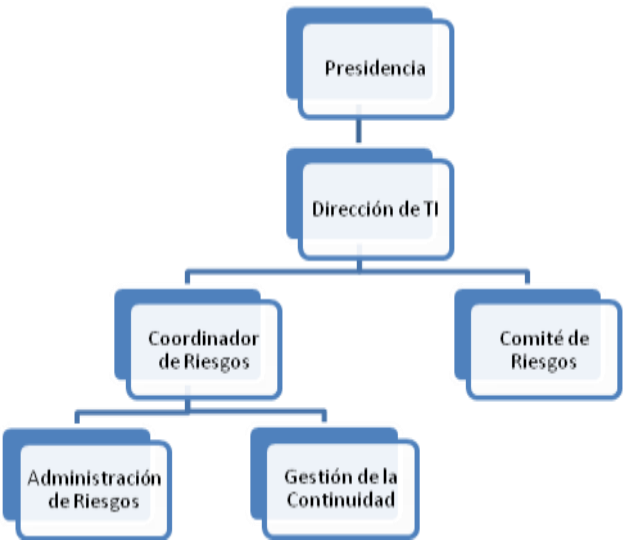
Negocio	saber: Lubricantes, Baterías y/o Dollarking
Revisoría Fiscal y Auditoría	Responsable del seguimiento y cumplimiento.

La estructura alcanzada para la unidad de Gestión de Riesgos de TI, es:

- ✓ El Director de TI quien además de las responsabilidades inherentes a la gestión de TI, asume la responsabilidad de la Unidad de Gestión de Riesgos de TI ante la Dirección del Negocio y su campo de acción está en el dominio del Gobierno de Riesgos.
- ✓ El Coordinador de Riesgos de TI quien se encargaría del liderazgo de todas las actividades Relacionadas en el campo de acción de los dominios de Administración, repuesta a riesgos y gestión de la continuidad de TI
- ✓ Un comité de Riesgos de TI el cual estaría conformado por la Dirección de TI, El coordinador de Riesgos de TI y representantes de cada una de las líneas de negocio. En este comité se revisan periódicamente la evaluación de riesgos, revisaran los procesos Relacionados con la unidad de gestión de riesgos y los proyectos de gestión de riesgos de TI. Actuarían en el dominio de Gobierno de Riesgos.

La estructura alcanzada para la unidad de Gestión de Riesgos de TI, durante el desarrollo de este proyecto, es:

FIGURA 90 – ORGANIGRAMA DE LA ESTRUCTURA ALCANZADA PARA LA UNIDAD DE GESTIÓN DE RIESGOS DE TI

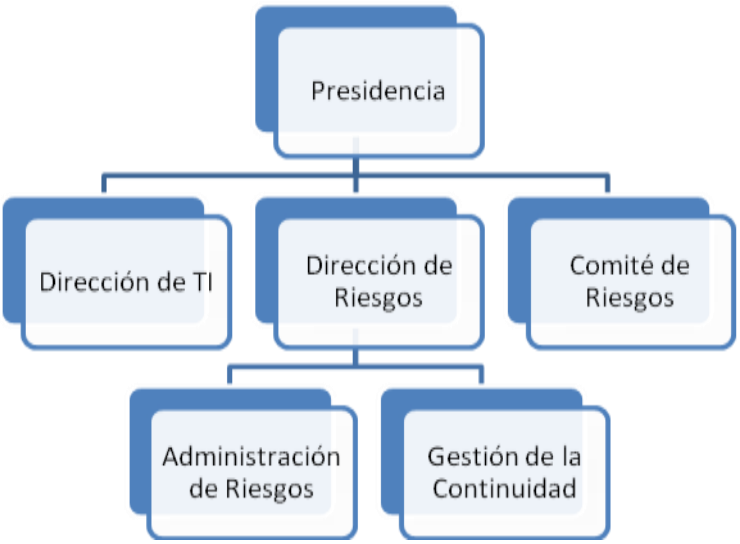


Como parte de la fase de implantación del marco de metodológico la estructura propuesta para la unidad de Gestión de Riesgos de TI, es:

- ✓ El Director de Riesgos asumirá la responsabilidad de la Unidad de Gestión de Riesgos de TI ante la Dirección del Negocio y su campo de acción está en el dominio del Gobierno de Riesgos, como una unidad independiente de TI y que reportará directamente a la Dirección del Negocio.
- ✓ El Coordinador de Gestión Riesgos de TI quien se encargaría del liderazgo de todas las actividades Relacionadas en el campo de acción de los dominios de Administración y repuesta a riesgos.
- ✓ El Coordinador de Gestión de la Continuidad que responderá por todo el proceso de gestión de la continuidad de TI: Planeación de la Continuidad, Administración de incidentes y la Administración de Crisis.
- ✓ El Director de TI quien responde por toda la gestión de TI de la organización, alineación de TI con las estrategias de negocio; planeación y administración de recursos, la entrega de servicios de TI y la administración del portafolio de TI.
- ✓ Un comité de Riesgos de TI el cual estaría conformado por la Dirección de TI, El coordinador de Riesgos de TI y representantes de cada una de las líneas de negocio. En este comité se revisan periódicamente la evaluación de riesgos, revisaran los procesos Relacionados con la unidad de gestión de riesgos y los proyectos de gestión de riesgos de TI. Actuarían en el dominio de Gobierno de Riesgos.

La estructura alcanzada para la unidad de Gestión de Riesgos de TI, durante el desarrollo de este proyecto, es:

FIGURA 21 – ORGANIGRAMA DE LA ESTRUCTURA PROPUESTA PARA LA UNIDAD DE GESTIÓN DE RIESGOS DE TI



10.4 MISION, FUNCIONES Y METAS DE LA UNIDAD DE GESTIÓN DE RIESGOS DE TI

Fundamentando nuestra propuesta en los principios de COSO ERM Framework [15] y el Marco de Trabajo RiskIT [7], la Misión de la Unidad de GERTI para el Grupo empresarial JADE comprende los siguientes aspectos:

- ✓ Proveer un lenguaje común alineado con el negocio para la gestión del riesgo.
- ✓ Proveer las políticas, procesos y procedimientos claros y costo-efectivos para la gestión de los riesgos de TI.

Seguimos el marco de Trabajo de RiskIT para establecer los procesos y metas de la Unidad de GERTI, así:

Procesos	Metas
✓ Establecer una mantener una visión común de los riesgos ✓ Integrar con la gestión del riesgo corporativa ✓ Tomar decisiones de negocio conscientes del riesgo.	Asegurar que las prácticas de gestión de riesgo de TI se integren con las demás áreas de la empresa, lo que permite asegurar un rendimiento ajustado con un riesgo óptimo.
✓ Recopilar datos e información de Riesgos ✓ Análisis de Riesgos ✓ Mantener el perfil de riesgos	Asegurar que los riesgos oportunidades de TI se identifican, analizan y se presentan en términos de negocio.
✓ Articular los Riesgos ✓ Administrar el riesgo. ✓ Reaccionar a eventos.	Asegurar que todos los casos, oportunidades y eventos Relacionados con riesgos de TI se direccionen con prácticas costo-efectiva y alineadas con las prioridades del negocio.

Se propone establecer como componentes básicos del accionar o estrategias de la Unidad de GERTI los siguientes:

- Difusión de las políticas, obligaciones y roles esperados de todos los involucrados en el Gobierno de la Gestión de Riesgos de TI.
- Capacitación y guía técnica en materia de prevención de riesgos de TI a todo nivel de la organización

- Estudio y adopción de estándares para asegurar el buen tratamiento de los eventos Relacionados con Riesgos de TI.
- Difusión de las recomendaciones y técnicas de prevención de Riesgos que resulten aconsejables o adecuadas.
- Institucionalización gradual de un sistema de reglamentaciones generales o particulares atendiendo a las condiciones o factores de riesgo.
- Realización y centralización de estadísticas normalizadas sobre eventos Relacionados con Riesgos de TI para el estudio de las causas determinantes y promover controles para disminuir el riesgo Residual.

11. BIBLIOGRAFÍA

[1] **Fuertes, Luis.** Gestión de riesgos TI. Cómo implantar las mejores prácticas. [En línea] 2010. [Citado el: 14 de Marzo de 2010]. http://www.aslan.es/boletin/boletin52/nuevoasociado.shtml.

[2] **SYMANTEC.** IT Risk Management Report 2: Myths and Realities. [En línea] 2010. [Citado el: 16 de Marzo de 2010]. https://www-935.ibm.com/services/es/cio/pdf/GESTIÓN-riesgos-ti-unos-sistemas-informacion-maduros-pueden-generar-grandes-resultados.pdf

[3] Presentación Corporativa. Barranquilla: s.n., 2008. 2.

[4] **Grupo Empresarial JADE.** *Documento Planeación Estratégica Corporativa.* Barranquilla : s.n., 2008.

[5] **Grupo Empresarial JADE, Gerente Administrativo Financiero.** *Entrevista Personal.* Agosto de 2009.

[6] 1 **OB/7, Joint Technichal Committee.** *Australian Standard. Risk Management.* Strathfield : Standard Asociation of Australia, 1999. Vol. AS/NZS 4360:1999.

[7] 2 **IT Governance Institute.** *ENTERPRISE RISK: IDENTIFY, GOVERN AND MANAGE IT RISK, The RiskIT Framework.* Rolling Meadows, IL 60008 USA: s.n., 2009.

[8] 3 **ICONTEC.** *Norma Técnica Colombiana NTC 5254, GESTIÓN de Riesgo.* Bogotá, Col.: s.n., 2006.

[9] 4 **IT Governance Institute.** *COBIT 4.0.* Rolling Meadows, IL EEUU : s.n., 2005.

[10] Instituto de Auditores internos de argentina. www.iaia.org.ar. [En línea] 2009.

[11] 7 **ISACA.** www.isaca.org. [En línea] 2009. [Citado el: 15 de Agosto de 2009.] http://www.isaca.org/Template.cfm?Section=Risk_IT&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749.

[12] 13. *IT Risk Exploration: The IT Risk Management.* **Schlarman, Steve.** s.l. : Isaca Journal, 2009.

[13] 11. **VanScoy, RogerL.** *SoftwareDevelopment Risk:Opportunity,Not Problem.* s.l. : SoftwareEngineering Institute, September, 1992. CMU/SEI-92-TR-30, ADA 258743.

[14] 9. *IT Governance on One Page.* **Weill, Peter y Ross, Jeanne W.** [ed.] Massachusetts Institue of Technology. Cambridge, Massachusetts : s.n., Noviembre de 2004, MIT Sloan Managemenst.

[15] 12. **Committee of sponsoring organizations of the treadway commission.** *Enterprise Risk Management. Integrated Framework.* 2004.

[16] 10. **IT Governance Institute.** *ENTERPRISE VALUE:GOVERNANCE OF IT INVESTMENTS. The Val IT Framework 2.0.* Rolling Meadows, IL 60008 USA : s.n., 2008.

[17] **IT Governance Institute.** *Los Objetivos de Control para la Información y la Tecnología Relacionada. The COBIT Framework 4.0.* Rolling Meadows, IL 60008 USA : s.n., 2005.

[18] 14. **MINTZBERG, Henry.** *Estructuras de organización ¿Por moda o por necesidad?* Buenos Aires : Biblioteca Harvard de Administración de Empresas, 1982. 330.